PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-138969
(43)Date of publication of application : 20.05.1994

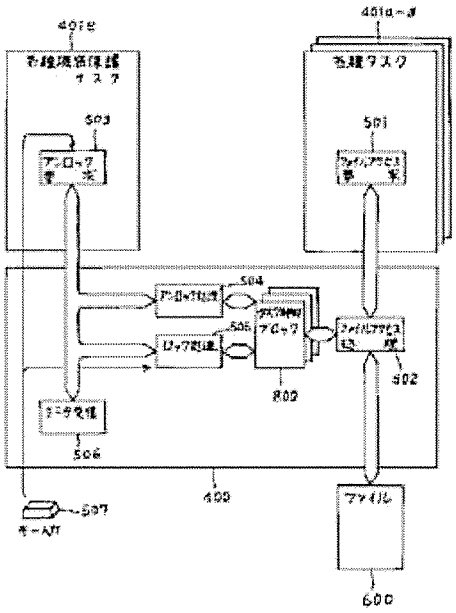
(51)Int.Cl. G06F 1/00
G06F 15/00

(21)Application number : 04-288399
(22)Date of filing : 27.10.1992

(71)Applicant : HITACHI LTD
(72)Inventor : KUWAMOTO HIDEKI
IWATANI TAKAO
OZAKI TOMOYA

(54) SECURITY SYSTEM

(57)Abstract:
PURPOSE: To prevent the illegal use of a file by setting a security state anytime when a user wants it.
CONSTITUTION: When various tasks 401 make an access to a file 600, a file access processing 502 called by a file access processing request 501 collates a user ID of the file 600 with the user ID of a task control block 800, limiting the access of the file 600 by the task 401 according to the file protection attribute of the file 600. An unlock processing 504 is called by an unlock request 503 of various security tasks 401e called by the direction of a user by key input 507 or the like and data reception 506 which directs unlocking, setting the user ID of the task control block 800. Thus, the illegal use of the file can be prevented.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平6－138969

(43)公開日　平成６年(1994)５月20日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　1/00	３７０　Ｅ	7165－5B		
15/00	３３０　Ａ	7459－5L		

審査請求　未請求　請求項の数29(全 26 頁)

(21)出願番号　特願平4－288399

(22)出願日　平成４年(1992)10月27日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　桑本　英樹
横浜市戸塚区吉田町292番地株式会社日立製作所マイクロエレクトロニクス機器開発研究所内

(72)発明者　岩谷　隆雄
横浜市戸塚区吉田町292番地株式会社日立製作所マイクロエレクトロニクス機器開発研究所内

(74)代理人　弁理士　小川　勝男

最終頁に続く

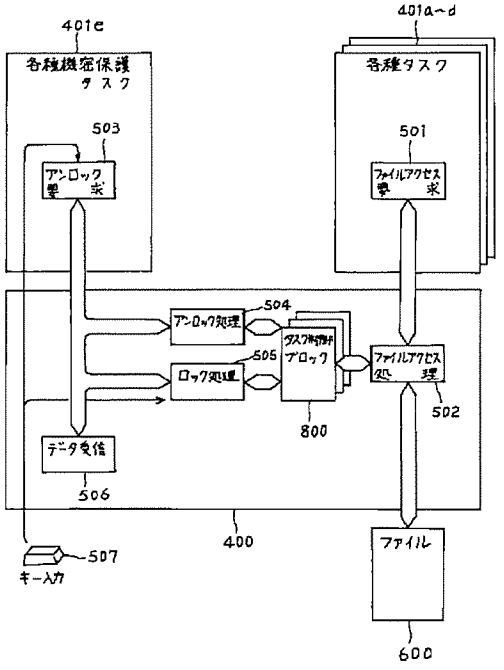
(54)【発明の名称】　機密保護方式

(57)【要約】

【目的】情報処理装置におけるファイルの不正利用を防止すること。

【構成】情報処理装置の利用者に対する機密保護状態の解除（アンロック）、及び、機密保護状態の設定（ロック）を、利用者が希望する任意の時点で行うことを可能にし、また、該情報処理装置が設置されている部屋への利用者の入退室や、該情報処理装置の操作の中断とリンクして、ロックとアンロックを行う。そして、ロックされている状態では、アクセスが禁止されているファイルのアクセスを禁止することで、ファイルの不正利用を防止することができる。

図５



1

【特許請求の範囲】

【請求項１】中央処理装置と記憶装置と入力装置と出力装置と通信装置からなる第１の情報処理装置と、その情報装置が設置されている部屋の入退室を管理するための、中央処理装置と記憶装置と入力装置と通信装置からなる第２の情報処理装置からなる情報処理システムにおいて、

該情報処理装置の利用者が該部屋への入室の通知を該第２の情報処理装置に入力する入力手段と、

該第２の情報処理装置が、該利用者の該部屋への入室の通知を入力されたならば、該利用者を識別する利用者識別子と入室であることを記した入室データを第１の情報処理装置に通知する入室データ送信手段と、

該第１の情報処理装置が該入室データを受信したならば、利用者の区別によって読書きが許可または不許可となるファイルに対して該入室データの利用者識別子に対応する利用者に許されるアクセスを、直ちに可能にする機密保護解除手段を有することを特徴とする機密保護方式。

【請求項２】中央処理装置と記憶装置と入力装置と出力装置と通信装置からなる第１の情報処理装置と、その情報装置が設置されている部屋の入退室を管理するための、中央処理装置と記憶装置と入力装置と通信装置からなる第２の情報処理装置からなるシステムにおいて、

該情報処理装置の利用者が該部屋からの退室の通知を該第２の情報処理装置に入力する入力手段と、

該第２の情報処理装置が、該利用者の該部屋からの退室の通知を入力されたならば、該利用者を識別する利用者識別子と退室であることを記した退室データを第１の情報処理装置に通知する退室データ送信手段と、

該第１の情報処理装置が該退室データを受信したならば、利用者の区別によってアクセスが許可または不許可となるファイルに対して該入室データの利用者識別子に対応する利用者に許されるアクセスを、直ちに解除する機密保護設定手段を有することを特徴とする機密保護方式。

【請求項３】中央処理装置と記憶装置と入力装置と出力装置と通信装置からなる第１の情報処理装置と、その情報装置が設置されている部屋の入退室を管理するための、中央処理装置と記憶装置と入力装置と通信装置からなる第２の情報処理装置からなるシステムにおいて、

該情報処理装置の利用者が該部屋への入室の通知を該第２の情報処理装置に入力する入力手段と、

該第２の情報処理装置が、該利用者の該部屋への入室の通知を入力されたならば、該利用者を識別する利用者識別子と入室であることを記した入室データを第１の情報処理装置に通知する入室データ送信手段と、

該情報処理装置で動作するタスクに、該タスクの起動を依頼した利用者を示す利用者識別子を対応づける手段と、

2

該第１の情報処理装置が該入室データを受信したならば、利用者の区別によってアクセスが許可または不許可となるファイルに対して該入室データの利用者識別子に対応する利用者に許されるアクセスが可能な状態を、該利用者識別子と同一の利用者識別子が対応づけられているタスクに直ちに設定する機密保護解除手段を有することを特徴とする機密保護方式。

【請求項４】中央処理装置と記憶装置と入力装置と出力装置と通信装置からなる第１の情報処理装置と、その情報装置が設置されている部屋の入退室を管理するための、中央処理装置と記憶装置と入力装置と通信装置からなる第２の情報処理装置からなるシステムにおいて、

該情報処理装置の利用者が該部屋からの退室の通知を該第２の情報処理装置に入力する入力手段と、

該情報処理装置で動作するタスクに、該タスクの起動を依頼した利用者を示す利用者識別子を対応づける手段と、

該第２の情報処理装置が、該利用者の該部屋からの退室の通知を入力されたならば、該利用者を識別する利用者識別子と退室であることを記した退室データを第１の情報処理装置に通知する退室データ送信手段と、

該第１の情報処理装置が該退室データを受信したならば、利用者の区別によってアクセスが許可または不許可となるファイルに対して該入室データの利用者識別子で示される利用者にのみ許されるアクセスが不可能な状態を、該利用者識別子と同一の利用者識別子が対応づけられているタスクに直ちに設定する機密保護設定手段を有することを特徴とする機密保護方式。

【請求項５】中央処理装置と記憶装置と入力装置と出力装置と通信装置からなる第１の情報処理装置と、その情報装置が設置されている部屋の入退室を管理するための、中央処理装置と記憶装置と入力装置と通信装置からなる第２の情報処理装置からなるシステムにおいて、

第１の情報処理装置に、

データの特定の利用者を識別する利用者識別子と、特定の利用者以外のアクセスを禁止するか否かを記述した保護属性と、データ本体とからなるデータと、

実行中の各タスクに対応して設け、該タスクの利用者を識別する利用者識別子を格納したタスク制御ブロックと、

利用者識別子と暗証番号の対応関係を記述した暗証番号管理テーブルと、

利用者が、他人へのアクセスを禁止したデータをアクセスするために、利用者識別子と暗証番号を用いて、該情報処理装置の該利用者に対する機密保護状態の解除を該情報処理装置に指示する第１の入力手段と、

利用者が、該情報処理装置を、他人のアクセスを禁止したデータへ他人がアクセスすることを禁止する状態にするために、第１の入力手段を用いた指示により解除された機密保護状態を解除前の状態に戻す、つまり、機密保

護状態を設定する指示を行う第２の入力手段と、
第１の入力手段による入力が行われたときに、利用者識別子と暗証番号の対応関係が、暗証番号管理テーブルに記述されている対応関係と一致するか否かを検査し、該検査が一致を示したならば、実行中のタスクに対応するタスク制御ブロックの利用者識別子フィールドに、指定された利用者識別子を記述する第１の制御手段と、
タスクがデータをアクセスする処理を実行する際に、アクセスするデータの利用者識別子とアクセスを行うタスクに対応するタスク制御ブロックの利用者識別子が一致するか否かを検査し、また、データの保護属性を参照して、利用者識別子が不一致かつ保護属性が特定の利用者以外のアクセスを禁止している場合は、該データへのアクセスを不許可と判定し、それ以外の場合は許可と判定し、アクセスが不許可の場合は該データをアクセスする処理を中止し、一方、許可された場合は、該データをアクセスする処理を続行する第２の制御手段と、
第２の入力手段により機密保護状態の設定の指示があったときに、実行中のタスクに対応するタスク制御ブロックの利用者識別子フィールドをクリア（一般の利用者を示す利用者識別子を格納する）する第３の制御手段と、
入退室を管理する第２の情報処理装置から、退室した利用者の利用者識別子が通知されたならば、実行中のタスクに対応するタスク制御ブロックで該利用者識別子と同一の利用者識別子が格納されている利用者識別子フィールドをクリア(一般の利用者を示す利用者識別子を格納する）する第４の制御手段と、
入退室を管理する第２の情報処理装置から、入室した利用者の利用者識別子が通知されたならば、実行中のタスクに対応するタスク制御ブロックの利用者識別子フィールドに該利用者識別子を格納する第５の制御手段とを設け、
第２の情報処理装置に、
入室する利用者の利用者識別子を入力する第１の入力手段と、
退室する利用者の利用者識別子を入力する第２の入力手段と、
入室する利用者の利用者識別子が第１の入力手段により入力されたならば、該利用者識別子の利用者識別子を入室した利用者の利用者識別子として、第１の情報処理装置に通知する第１の制御手段と、
退室する利用者の利用者識別子が第２の入力手段により入力されたならば、該利用者の利用者識別子を退室した利用者の利用者識別子として、第１の情報処理装置に通知する第２の制御手段とを設けたことを特徴とする機密保護方式。
【請求項６】中央処理装置と記憶装置と入力装置と出力装置と通信装置からなる第１の情報処理装置と、その情報装置が設置されている部屋の入退室を管理するための、中央処理装置と記憶装置と入力装置と通信装置からなる第２の情報処理装置からなるシステムにおいて、

第１の情報処理装置に、
データの特定の利用者を識別する利用者識別子と、特定の利用者以外のアクセスを禁止するか否かを記述した保護属性と、データ本体とからなるデータと、
実行中の各タスクに対応して設け、該タスクの利用者を識別する利用者識別子を格納したタスク制御ブロックと、
利用者識別子と暗証番号の対応関係を記述した暗証番号管理テーブルと、
利用者が、他人へのアクセスを禁止したデータをアクセスするために、利用者識別子と暗証番号を用いて、該情報処理装置の該利用者に対する機密保護状態の解除を該情報処理装置に指示する第１の入力手段と、
第１の入力手段による入力が行われたときに、利用者識別子と暗証番号の対応関係が、暗証番号管理テーブルに記述されている対応関係と一致するか否かを検査し、該検査が一致を示したならば、実行中のタスクに対応するタスク制御ブロックの利用者識別子フィールドに、指定された利用者識別子を記述する第１の制御手段と、
タスクがデータをアクセスする処理を実行する際に、アクセスするデータの利用者識別子とアクセスを行うタスクに対応するタスク制御ブロックの利用者識別子が一致するか否かを検査し、また、データの保護属性を参照して、利用者識別子が不一致かつ保護属性が特定の利用者以外のアクセスを禁止している場合は、該データへのアクセスを不許可と判定し、それ以外の場合は許可と判定し、アクセスが不許可の場合は該データをアクセスする処理を中止し、一方、許可された場合は、該データをアクセスする処理を続行する第２の制御手段と、
入退室を管理する第２の情報処理装置から、入室した利用者の利用者識別子が通知されたならば、実行中のタスクに対応するタスク制御ブロックの利用者識別子フィールドに該利用者識別子を格納する第４の制御手段とを設け、
第２の情報処理装置に、
入室する利用者の利用者識別子を入力する第１の入力手段と、
入室する利用者の利用者識別子が第１の入力手段により入力されたならば、該利用者の利用者識別子を入室した利用者の利用者識別子として、第１の情報処理装置に通知する第１の制御手段とを設けたことを特徴とする機密保護方式。
【請求項７】中央処理装置と記憶装置と入力装置と出力装置と通信装置からなる第１の情報処理装置と、その情報装置が設置されている部屋の入退室を管理するための、中央処理装置と記憶装置と入力装置と通信装置からなる第２の情報処理装置からなるシステムにおいて、
第１の情報処理装置に、
データの特定の利用者を識別する利用者識別子と、特定

5

の利用者以外のアクセスを禁止するか否かを記述した保護属性と、データ本体とからなるデータと、
実行中の各タスクに対応して設け、該タスクの利用者を識別する利用者識別子を格納したタスク制御ブロックと、
利用者識別子と暗証番号の対応関係を記述した暗証番号管理テーブルと、
利用者が、該情報処理装置を、他人のアクセスを禁止したデータへ他人がアクセスすることを禁止する状態にするために、第１の入力手段を用いた指示により解除された機密保護状態を解除前の状態に戻す、つまり、機密保護状態を設定する指示を行う第２の入力手段と、
タスクがデータをアクセスする処理を実行する際に、アクセスするデータの利用者識別子とアクセスを行うタスクに対応するタスク制御ブロックの利用者識別子が一致するか否かを検査し、また、データの保護属性を参照して、利用者識別子が不一致かつ保護属性が特定の利用者以外のアクセスを禁止している場合は、該データへのアクセスを不許可と判定し、それ以外の場合は許可と判定し、アクセスが不許可の場合は該データをアクセスする処理を中止し、一方、許可された場合は、該データをアクセスする処理を続行する第１の制御手段と、
第２の入力手段により機密保護状態の設定の指示があったときに、実行中のタスクに対応するタスク制御ブロックの利用者識別子フィールドをクリア（一般の利用者を示す利用者識別子を格納する）する第３の制御手段と、
入退室を管理する第２の情報処理装置から、退室した利用者の利用者識別子が通知されたならば、実行中のタスクに対応するタスク制御ブロックで該利用者識別子と同一の利用者識別子が格納されている利用者識別子フィールドをクリア（一般の利用者を示す利用者識別子を格納する）する第５の制御手段と、
第２の情報処理装置に、
退室する利用者の利用者識別子を入力する第２の入力手段と、
退室する利用者の利用者識別子が第２の入力手段により入力されたならば、該利用者の利用者識別子を退室した利用者の利用者識別子として、第１の情報処理装置に通知する第２の制御手段とを設けたことを特徴とする機密保護方式。
【請求項８】請求項２又は４記載の機密保護方式において、
該第１の情報処理装置が該退室データを受信したならば、利用者の区別によってアクセスが許可または不許可となるファイルに対して、該退室データの利用者識別子で示される利用者に許されるアクセスが可能な状態を、オープン中のファイルがクローズした時点で直ちに解除する機密保護設定手段を有することを特徴とする機密保護方式。
【請求項９】請求項５又は７記載の機密保護方式において、

6

実行中の各タスクに対応して設け、該タスクの利用者を唯一に識別する利用者識別子を格納したタスク制御予備ブロックを設け、
第４の制御手段の代わりに、入退室を管理する第２の情報処理装置から、退室した利用者の利用者識別子が通知されたならば、実行中のタスクに対応するタスク制御予備ブロックで該利用者識別子と同一の利用者識別子が格納されている利用者識別子フィールドをクリア（一般の利用者を示す利用者識別子を格納する）する第４Ａの制御手段を設け、
オープン中のファイルがクローズした時点で、該ファイルをオープンしていたタスクに対応するタスク制御予備ブロックの利用者識別子を、該タスクに対応するタスク制御ブロックに直ちに格納する第４Ｂの制御手段を設けたことを特徴とする機密保護方式。
【請求項１０】請求項１又は３記載の機密保護方式において、
利用者の区別によってアクセスが許可または不許可となるファイルに対して該入室データの利用者識別子に対応する利用者に許されるアクセスが可能な状態を該利用者識別子と同一の利用者識別子が対応づけられているタスクに設定する際は、その時点で既に該タスクに設定されている特定の利用者がアクセスが可能な状態を保持しながら、追記して設定することを特徴とする機密保護方式。
【請求項１１】請求項１０記載の機密保護方式において、
利用者の区別によってアクセスが許可または不許可となるファイルに対して該入室データの利用者識別子に対応する利用者に許されるアクセスが不可能な状態を該利用者識別子と同一の利用者識別子が対応づけられているタスクに設定する際は、該利用者に対してのみ該不可能な状態を該タスクに設定することを特徴とする機密保護方式。
【請求項１２】請求項５又は６記載の機密保護方式において、
タスク制御ブロックは、該タスクの利用者を識別する利用者識別子を複数格納可能とし、
第１の制御手段は、第１の入力手段による入力が行われたときに、利用者識別子と暗証番号の対応関係が、暗証番号管理テーブルに記述されている対応関係と一致するか否かを検査し、該検査が一致を示したならば、タスク制御ブロックの利用者識別子フィールドに、その時点で既に該タスク制御ブロックの該利用者識別子フィールドに設定されている利用者識別子を保持しながら、追記して指定された利用者識別子を格納し、
第４の制御手段は、入退室を管理する第２の情報処理装置から、入室した利用者の利用者識別子が通知されたならば、タスク制御ブロックの利用者識別子フィールド

に、その時点で既に該タスク制御ブロックの該利用者識別子フィールドに設定されている利用者識別子を保持しながら、追記して指定された利用者識別子を格納することを特徴とする機密保護方式。

【請求項１３】請求項５又は７記載の機密保護方式において、

第２の入力手段は、機密保護状態に戻したい利用者の利用者識別子をともに、入力し、

第３の制御手段は、第２の入力手段により機密保護状態の設定が、利用者識別子とともに指示されたときに、指定された利用者識別子と同一の利用者識別子が格納されているタスク制御ブロックの利用者識別子フィールドをクリア（一般の利用者を示す利用者識別子を格納する）し、

第５の制御手段は、入退室を管理する第２の情報処理装置から、退室した利用者の利用者識別子が通知されたならば、タスク制御ブロックで該利用者識別子と同一の利用者識別子が格納されている利用者識別子フィールドをクリア（一般の利用者を示す利用者識別子を格納する）することを特徴とする機密保護方式。

【請求項１４】請求項２，４，５，７，８又は９記載の機密保護方式において、

タスク制御ブロックまたはタスク制御予備ブロックの利用者識別子フィールドをクリア（一般の利用者を示す利用者識別子を格納する）する制御は、予め定められている画面を出力装置に表示することによって起動する手段を設けたことを特徴とする機密保護方式。

【請求項１５】請求項１４記載の機密保護方式において、

タスク制御ブロックまたはタスク制御予備ブロックの利用者識別子フィールドをクリア（一般の利用者を示す利用者識別子を格納する）する制御は、予め定められている画面を予め定められている一定時間出力装置に表示した後に起動する手段を設けたことを特徴とする機密保護方式。

【請求項１６】請求項２，４，５，７，８又は９記載の機密保護方式において、

タスク制御ブロックまたはタスク制御予備ブロックの利用者識別子フィールドをクリア（一般の利用者を示す利用者識別子を格納する）する制御は、予め定められている入力装置からの入力において、無入力の時間が予め定められている一定時間に達した時点で起動する手段を設けたことを特徴とする機密保護方式。

【請求項１７】請求項２，４，５，７，８又は９記載の機密保護方式において、

スクリーンセーバ手段を設け、

タスク制御ブロックまたはタスク制御予備ブロックの利用者識別子フィールドをクリアする制御は、スクリーンセーバが機能した時点で起動する手段を設けたことを特徴とする機密保護方式。

【請求項１８】請求項２，４，５，７，８又は９記載の機密保護方式において、

該情報処理装置を操作する利用者が、該情報処理装置の操作を中止し、該情報処理装置から離れた離席を検出する離席検出手段を設け、

タスク制御ブロックまたはタスク制御予備ブロックの利用者識別子フィールドをクリアする制御は、離席検出手段により離席が検出された時点で起動する手段を設けたことを特徴とする機密保護方式。

【請求項１９】請求項１２又は１３記載の機密保護方式において、

データにおいて特定の利用者以外のアクセスを禁止するか否かを記述した保護属性には、該利用者を識別する複数の利用者識別子と、該複数の利用者に許可されるアクセスの種類（読込み，書込み，実行）と、全ての該複数の利用者の利用者識別子が本データのアクセスを行うタスクのタスク制御ブロックに記述されている場合のみ該アクセスを許可する（連動）か否か（非連動）を記述した連動識別子とを設け、

第２の制御手段は、タスクがデータをアクセスする処理を実行する際に、データの保護属性において何れかのアクセスの種類（読込み，書込み，実行）が不許可とされている場合は、データの保護属性の連動識別子が連動を示していたならば、アクセスするデータの保護属性に記述されている全ての利用者識別子について、一致する利用者識別子がアクセスを行うタスクに対応するタスク制御ブロックに格納されている場合のみ該データへのアクセスを許可と判定し、データの保護属性の連動識別子が非連動を示していたならば、アクセスするデータの保護属性に記述されている何れかの利用者識別子と一致する利用者識別子がアクセスを行うタスクに対応するタスク制御ブロックに格納されている場合に該データへのアクセスを許可と判定し、一方、データの保護属性において、全てのアクセスの種類（読込み，書込み，実行）が許可されている場合は、該データへのアクセスを許可と判定し、その結果、アクセスが不許可の場合は該データをアクセスする処理を中止し、一方、許可された場合は、該データをアクセスする処理を続行することを特徴とする機密保護方式。

【請求項２０】請求項６記載の機密保護方式において、

タスク制御ブロックは、実行中の各タスクに対応して設け、該タスクの利用者を識別する利用者識別子と、該利用者識別子が有効か無効かを記述した識別子有効フラグを格納し、

第１の制御手段は、第１の入力手段による入力が行われたときに、利用者識別子と暗証番号の対応関係が、暗証番号管理テーブルに記述されている対応関係と一致するか否かを検査し、該検査が一致を示したならば、実行中のタスクに対応するタスク制御ブロックの利用者識別子フィールドに、指定された利用者識別子を記述し、ま

た、該利用者識別子に対応する識別子有効フラグを有効に設定し、

第２の制御手段は、タスクがデータをアクセスする処理を実行する際に、アクセスするデータの利用者識別子と、アクセスを行うタスクに対応するタスク制御ブロックにおける識別子有効フラグが有効である利用者識別子とが一致するか否かを検査し、また、データの保護属性を参照して、利用者識別子が不一致かつ保護属性が特定の利用者以外のアクセスを禁止している場合は、該データへのアクセスを不許可と判定し、それ以外の場合は許可と判定し、アクセスが不許可の場合は該データをアクセスする処理を中止し、一方、許可された場合は、該データをアクセスする処理を続行し、

第４の制御手段、入退室を管理する第２の情報処理装置から、入室した利用者の利用者識別子が通知されたならば、タスク制御ブロックにおいて該利用者識別子と同一の利用者識別子に対応する識別子有効フラグに有効を設定することを特徴とする機密保護方式。

【請求項２１】請求項７記載の機密保護方式において、

第３の制御手段は、第２の入力手段により機密保護状態の設定の指示があったときに、実行中のタスクに対応するタスク制御ブロックの利用者識別子フィールドをクリア（一般の利用者を示す利用者識別子を格納し）し、また、識別子有効フラグに無効を設定し、

第２の制御手段は、タスクがデータをアクセスする処理を実行する際に、アクセスするデータの利用者識別子と、アクセスを行うタスクに対応するタスク制御ブロックにおける識別子有効フラグが有効である利用者識別子とが一致するか否かを検査し、また、データの保護属性を参照して、利用者識別子が不一致かつ保護属性が特定の利用者以外のアクセスを禁止している場合は、該データへのアクセスを不許可と判定し、それ以外の場合は許可と判定し、アクセスが不許可の場合は該データをアクセスする処理を中止し、一方、許可された場合は、該データをアクセスする処理を続行し、

第５の制御手段は、入退室を管理する第２の情報処理装置から、退室した利用者の利用者識別子が通知されたならば、実行中のタスクに対応するタスク制御ブロックで該利用者識別子と同一の利用者識別子が格納されている利用者識別子フィールドに対応する識別子有効フラグを無効に設定することを特徴とする機密保護方式。

【請求項２２】請求項５又は６記載の機密保護方式において、

第２の情報処理装置に、特定の一つ以上の情報処理装置を示す装置識別子を格納する装置識別子管理テーブルを設け、

第２の情報処理装置の第１の制御手段は、該装置識別子管理テーブルに格納されている装置識別子に対応する情報処理装置へのみ、利用者識別子を第１の情報処理装置に通知することを特徴とする機密保護方式。

【請求項２３】請求項２２記載の機密保護方式において、

装置識別子管理テーブルに格納されている装置識別子に対応する情報処理装置は、特定の部屋内に格納されている情報処理装置であることを特徴とする機密保護方式。

【請求項２４】請求項２２記載の機密保護方式において、

有線通信を介して他の情報処理装置から受信したデータを無線通信を介して他の情報処理装置へ伝送し、無線通信を介して他の情報処理装置から受信したデータを有線通信を介して他の情報処理装置へ伝送する無線通信装置の装置識別子をデータ装置識別子管理テーブルに格納し、第２の情報処理装置からのデータの送受信を該無線通信装置からの電波の到達範囲に限定することを特徴とする機密保護方式。

【請求項２５】請求項２４記載の機密保護方式において、

部屋の外部への電波の漏洩を防止した部屋の内部に該無線通信装置を設置し、第２の情報処理装置からのデータの送受信を該部屋内に限定することを特徴とする機密保護方式。

【請求項２６】請求項５，６又は７記載の機密保護方式において、

第２の情報処理装置は出退勤管理を行う装置であり、出勤は入室に、退勤は退室に対応することを特徴とする機密保護方式。

【請求項２７】請求項５又は６記載の機密保護方式において、

第１の入力手段の入力を行うための専用のキーを設けたことを特徴とする機密保護方式。

【請求項２８】請求項５又は７記載の機密保護方式において、

第２の入力手段の入力を行うために専用のキーを設けたことを特徴とする機密保護方式。

【請求項２９】請求項１９記載の機密保護方式において、

データの保護属性は、連動／非連動の区別を記載した連動識別子を複数記載し、また、該各連動識別子に対応するアクセスの種類（読込み，書込み，実行）と一つ以上の利用者識別子を記載し、

第２の制御手段は、まず、各連動識別子毎に、各連動識別子に対応した利用者識別子とアクセス種類（読込み，書込み，実行）を用いてアクセスの許可／不許可の判定を行い、次に、各連動識別子に対応する結果の論理和でアクセスの許可／不許可を判定することを特徴とする機密保護方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は機密保護機能を有する情報処理装置に係り、特に該不特定多数の利用者が使用す

11

る機会の多い情報処理装置において、特定のデータまたは機能に対する特定の利用者以外のアクセスを制限する場合に好敵な機密保護方式及び装置に関する。

【０００２】

【従来の技術】情報処理装置において、特定のデータにおける特定の利用者以外のアクセスを制限する機密保護機能を設けることが広く普及している。

【０００３】従来の情報処理装置における機密保護機能の第１の従来例としては、特開昭６３－２４９２５４号において示されているようなものがある。すなわち、利用者が情報処理装置を使用するとき、該利用者氏名と暗証番号を入力する。そして、情報処理装置が該利用者氏名と暗証番号の対応関係の一致を確認した後、該利用者は該情報処理の使用が可能となる。このように、利用者を唯一に識別する番号または文字列と、該利用者に対応する暗証番号または文字列を入力することにより、情報処理の使用が可能となる方式は、端末装置で広く用いられている。

【０００４】前述の従来例は、情報処理装置の利用開始時に利用者氏名，暗証番号等を入力し、特定のデータへのアクセスが可能となる方式であるが、次に示すような第２の従来例もある。つまり、利用者が特定のデータまたは機能へのアクセスを情報処理装置に指示する毎に、該情報処理装置が暗証番号等の入力を該利用者に要求する方式である。

【０００５】また、情報処理システムの安全性を高める他の方法として、情報処理装置が設置されている部屋への入退室を管理するものがある。一般には、利用者ＩＤや暗証番号が記録されているカードを、部屋の出入口に設置されているカードリーダに読み取らせることにより、該出入口の施錠を解除するものである。これにより、該部屋への入室を該カード保有者のみに限定し、他の利用者の情報処理装置の不正利用を防止して、システムの安全性を高めるものである。

【０００６】

【発明が解決しようとする課題】上記の第１の従来技術においては、次のような問題点がある。つまり、その情報処理装置を使用しようとする全ての利用者は、利用者氏名，暗証番号等の何らかの入力を行う必要があり、不特定の一般利用者に簡単な操作を提供するのに障害となるという問題点である。特に、該情報処理装置の大部分の利用者は不特定の一般利用者であり、かつ、該情報処理装置には、機密性のあるデータ等特定の利用者のアクセスのみが許されるデータまたは機能が存在する場合には、一般の利用者に適した簡単な操作と、特定の利用者に適した簡単な操作を両立することが難しかった。また、第２の従来技術では、利用者は、特定のアクセスを行う毎に暗証番号等の入力を必要としているので、該情報処理装置を利用する作業の中で、特定のデータまたは機能へのアクセスと、一般のデータまたは機能へのアクセスとを頻繁に交互に繰り返す場合は、暗証番号等の入力も繰り返す必要があり、操作が煩雑になるという問題点があった。

12

【０００７】また、近年、従来のように情報処理装置を集中して特定の部屋に設置する使用形態は少なくなり、情報処理装置は一般オフィス内に分散して設置されるようになってきた。よって、部屋への入退室を管理しても、情報処理装置を操作しない人々の入室も数多く許可せざるを得なく、それらの人々による情報処理装置の不正使用が為される可能性が否定できないという問題点がある。

【０００８】また、複数の業務グループに属する人が情報処理装置の操作をする場合、従来は、同時に複数の業務グループの利用者ＩＤで情報処理装置を操作することが不可能という問題点があった。従来は、グループＩＤ等の階層的なＩＤを導入することによりこの問題点を解決していたが、利用者の所属変更が頻繁に行われる場合は、一人の利用者が複数の利用者ＩＤを持つことが実際には多くある。

【０００９】本発明は、かかる従来の問題点を解決し、特定の利用者のアクセスのみが許されるデータまたは機能を使用する利用者に適した簡便な操作と、利用者によるアクセスの制限がないデータまたは機能を使用する一般利用者に適した簡便な操作とを両立した機密保護機能の操作方法を実現し、さらに、その機密保護機能を部屋への入退室管理と連携させ、退室した利用者ＩＤによる情報処理装置の不正使用を防止することにある。

【００１０】

【課題を解決するための手段】上記目的は、中央処理装置と記憶装置と入力装置と出力装置からなる第１の情報処理装置と、入退室管理を行うための第２の情報処理装置からなるシステムにおいて、次に述べる手段を設けることにより達成される。

【００１１】まず、第１の情報処理装置に以下の手段を設ける。

【００１２】（１）データの所有者を識別する利用者識別子と、所有者以外のアクセスを禁止するか否かを記述した保護属性と、データ本体とからなるデータ。

【００１３】（２）実行中の各タスクに対応して設け、該タスクの利用者を唯一に識別する利用者ＩＤを格納したタスク制御ブロック。

【００１４】（３）利用者ＩＤと暗証番号の対応関係を記述した暗証番号管理テーブル。

【００１５】（４）利用者が、他人へのアクセスを禁止したデータをアクセスするために、利用者ＩＤと暗証番号を用いて、該情報処理装置の該利用者に対する機密保護状態の解除（アンロック）を該情報処理装置に指示する第１の入力手段。

【００１６】（５）利用者が、該情報処理装置を、他人のアクセスを禁止したデータへ他人がアクセスすること

を禁止する状態にするために、第１の入力手段を用いた指示により解除された機密保護状態を解除前の状態に戻す、つまり、機密保護状態を設定する（ロック）指示を行う第２の入力手段。

【００１７】（６）第１の入力手段による入力が行われたときに、利用者ＩＤと暗証番号の対応関係が、暗証番号管理テーブルに記述されている対応関係と一致するか否かを検査し、該検査が一致を示したならば、実行中のタスクに対応するタスク制御ブロックの利用者ＩＤフィールドに、指定された利用者ＩＤを記述する第１の制御手段。

【００１８】（７）タスクがデータをアクセスする処理を実行する際に、アクセスするデータの利用者ＩＤとアクセスを行うタスクに対応するタスク制御ブロックの利用者ＩＤが一致するか否かを検査し、また、データの保護属性を参照して、利用者ＩＤが不一致かつ保護属性が所有者以外のアクセスを禁止している場合は、該データへのアクセスを不許可と判定し、それ以外の場合は許可と判定し、アクセスが不許可の場合は該データをアクセスする処理を中止し、一方、許可された場合は、該データをアクセスする処理を続行する第２の制御手段。

【００１９】（８）第２の入力手段により機密保護状態の設定（ロック）の指示があったときに、実行中のタスクに対応するタスク制御ブロックの利用者ＩＤフィールドをクリア（一般の利用者を示す利用者ＩＤを格納する）する第３の制御手段。

【００２０】（９）入退室を管理する第２の情報処理装置から、退室した利用者の利用者ＩＤが通知されたならば、実行中のタスクに対応するタスク制御ブロックで該利用者ＩＤと同一の利用者Ｉが格納されている利用者ＩＤフィールドをクリア（一般の利用者を示す利用者ＩＤを格納する）する第４の制御手段。

【００２１】（１０）入退室を管理する第２の情報処理装置から、入室した利用者の利用者ＩＤが通知されたならば、実行中のタスクに対応するタスク制御ブロックの利用者ＩＤフィールドに該利用者ＩＤを格納する第５の制御手段。

【００２２】次に、第２の情報処理装置に以下の手段を設ける。

【００２３】（１１）入室する利用者の利用者ＩＤを入力する第１の入力手段。

【００２４】（１２）退室する利用者の利用者ＩＤを入力する第２の入力手段。

【００２５】（１３）入室する利用者の利用者ＩＤが第１の入力手段により入力されたならば、該利用者ＩＤの利用者ＩＤを入室した利用者の利用者ＩＤとして、第１の情報処理装置に通知する第１の制御手段。

【００２６】（１４）退室する利用者の利用者ＩＤが第２の入力手段により入力されたならば、該利用者ＩＤの利用者ＩＤを退室した利用者の利用者ＩＤとして、第１の情報処理装置に通知する第２の制御手段。

【００２７】

【作用】第１の情報処理装置において、利用者が、第１の入力手段により、他人へのアクセスを禁止したデータをアクセスするために、利用者ＩＤと暗証番号を用いて、該情報処理装置の該利用者に対する機密保護状態の解除（アンロック）を該情報処理装置に指示したならば、第１の制御手段により、利用者ＩＤと暗証番号の対応関係が、暗証番号管理テーブルに記述されている対応関係と一致するか否かを検査し、該検査が一致を示したならば、実行中のタスクに対応するタスク制御ブロックの利用者ＩＤフィールドに、指定された利用者ＩＤを記述する。

【００２８】また、第１の情報処理装置において、利用者が、第２の入力手段により、該情報処理装置を、他人のアクセスを禁止したデータへ他人がアクセスすることを禁止する状態にするために、第１の入力手段を用いた指示により解除された機密保護状態を解除前の状態に戻す、つまり、機密保護状態を設定する（ロック）指示を行ったならば、第３の制御手段により、実行中のタスクに対応するタスク制御ブロックの利用者ＩＤフィールドをクリア（一般の利用者を示す利用者ＩＤを格納する）する。

【００２９】また、第１の情報処理装置において、タスクがデータをアクセスする処理を実行する際には、第２の制御手段により、アクセスするデータの利用者ＩＤとアクセスを行うタスクに対応するタスク制御ブロックの利用者ＩＤが一致するか否かを検査し、また、データの保護属性を参照して、利用者ＩＤが不一致かつ保護属性が所有者以外のアクセスを禁止している場合は、該データへのアクセスを不許可と判定し、それ以外の場合は許可と判定し、アクセスが不許可の場合は該データをアクセスする処理を中止し、一方、許可された場合は、該データをアクセスする処理を続行する。

【００３０】また、第１の情報処理装置において、入退室を管理する第２の情報処理装置から、退室した利用者の利用者ＩＤが通知されたならば、第４の制御手段により、実行中のタスクに対応するタスク制御ブロックで該利用者ＩＤと同一の利用者Ｉが格納されている利用者ＩＤフィールドをクリア（一般の利用者を示す利用者ＩＤを格納する）する。

【００３１】また、第１の情報処理装置において、入退室を管理する第２の情報処理装置から、入室した利用者の利用者ＩＤが通知されたならば、第５の制御手段により、実行中のタスクに対応するタスク制御ブロックの利用者ＩＤフィールドに該利用者ＩＤを格納する。

【００３２】また、第２の情報処理装置において、入室する利用者の利用者ＩＤが第１の入力手段により入力されたならば、第１の制御手段により、該利用者ＩＤの利用者ＩＤを入室した利用者の利用者ＩＤとして、第１の

15

情報処理装置に通知する。

【００３３】また、第２の情報処理装置において、退室する利用者の利用者ＩＤが第２の入力手段により入力されたならば、第２の制御手段により、該利用者ＩＤの利用者ＩＤを退室した利用者の利用者ＩＤとして、第１の情報処理装置に通知する。

【００３４】このように、特定の利用者のアクセスのみが許されるデータまたは機能を使用する利用者に適した簡便な操作と、利用者によるアクセスの制限がないデータまたは機能を使用する一般利用者に適した簡便な操作とを両立した機密保護機能の操作方法を実現し、さらに、その機密保護機能を部屋への入退室管理と連携させ、退室した利用者ＩＤによる情報処理装置の不正使用を防止することができる。

【００３５】

【実施例】以下、本発明の一実施例を図面を用いて説明する。

【００３６】まず、図１と図２を用いて本システム構成と使用環境を説明する。１００は情報処理装置を設置または使用する部屋であり、電波を遮断する素材を用いた構造となっている。該部屋１００の入口１０１には、部屋の内側と外側に入退室管理装置１１１がある。該部屋内には、情報処理装置１１０と無線ＬＡＮ制御装置１１２が設けられている。各情報処理装置１１０、入退室管理装置１１１、無線ＬＡＮ制御装置１１２は、互いにＬＡＮ１１３または無線通信により接続されていて、各装置１１０～１１２間でのデータ通信が可能である。なお、無線通信は、無線ＬＡＮ制御装置１１２と無線通信用のアンテナをもつ該部屋内にある情報処理装置１１０ｃの間で行われる。無線ＬＡＮ制御装置１１２は、部屋の外にある情報処理装置１１０ｃとの間では通信を行うことができない。各装置１１０～１１２は、ディスプレイ装置や通信装置の有無という多少の差があるが、ほぼ同一のハードウェア構成を有する。なお、入退室管理装置１１１は、部屋の内部に設けられるカードリーダ１１１ａと、部屋の外部に設けられるカードリーダ１１１ｂが接続される。カードリーダ１１１ａ，ｂは、カード１１４へのデータの書き込みまたは読み出しが可能である。

【００３７】次に、図３を用いて、各装置１１０～１１２のハードウェア構成について説明する。３０１は中央処理ユニット（ＣＰＵ）であり、各種の処理プログラムの実行、及び周辺機器３０２～３０９の制御を行なう。３０２は主メモリ（Ｍ）であり、機密保護機能を初めとする各種の処理プログラム及びデータが格納される。機密保護機能を初めとする各種の処理プログラムに対する指示は、キーボード３０６（ＫＢ）、マウス３０７を介して行なわれる。３０５はディスプレイ装置(Ｄ）であり、機密保護機能を初めとする各種の処理プログラムに関する画面をマルチウインドウの形式で表示する。３０４はフロッピディスク装置（ＦＤＤ）であり、各種のデータの読み出しや保存を行なう。３０３は固定ディスク装置（ＨＤＤ）であり、各種のデータの読み出しまたは保存を行なう。３１０はこれらの周辺機器３０２～３０９と中央処理ユニット３０１間のデータ転送を行なうためのバスである。

16

【００３８】次に、図４を用いて、本実施例のソフトウェア構成について説明する。４０１ａ～ｅは、本実施例の情報処理装置に各種の処理タスクである。４０１ａ～ｅは各々独立したタスクとしてマルチタスクオペレーティングシステムプログラム(以下ＯＳと略す）４００で制御される。また、タスク４０１ｅは機密保護機能に係るタスクである。ＯＳ４００は、基本的なタスク制御や入出力制御から、ディスプレイ装置３０５の画面上でマルチウインドウを実現する制御、後で述べるファイルをアクセスする制御、機密保護機能に係る制御等を行う。

【００３９】次に、図５を用いて、本実施例の情報処理装置における機密保護機能の処理機構について説明する。機密保護機能は、情報処理装置１１０上で動作する各種のタスク４０１が、固定ディスク装置３０３に格納されているファイル６００をアクセスする場合に、タスク４０１のファイルアクセス要求処理５０１によって呼び出されたＯＳ４００のファイルアクセス処理５０２が、ファイル６００の利用者ＩＤ６３０とタスク制御ブロック８００の利用者ＩＤ８１０の照合を行い、ファイル６００のファイル保護属性６３０に従って、タスク４０１によるファイル６００のアクセスを制限するものである。そして、タスク制御ブロック８００の利用者ＩＤ８１０は、キー入力５０７等の利用者の指示によって呼び出された各種の機密保護タスク４０１ｅのアンロック要求５０３や、アンロックを指示するデータの受信５０６等により、ＯＳ４００のアンロック処理５０４が呼出され、該アンロック処理５０４がタスク制御ブロック８００の利用者ＩＤ８１０を設定する。なお、キー５０７は、キーボード３０６に設けられているものであり、アンロック等の機密保護機能を起動ための専用キーである。キー５０７には、アンロックを指定する専用キー５０７ａとロックを指定する専用キー５０７ｂがそれぞれ設けられている。専用キーを設けることにより、利用者はアンロック，ロックの機能を容易に発見することができ、よって、利用機会が増加かつ普及するとともに、瞬時に該機能を起動することができる。

【００４０】次に、図６と図７を用いて、本実施例に係るファイルのデータ構造について説明する。ファイル６００は、ファイル名称６１０、ファイル保護属性６２０、利用者ＩＤ６３０、及びデータ６４０からなり、各種のデータや実行可能な処理プログラムが格納される。ファイル名称６１０は、該ファイル６００の名称を示す。ファイル保護属性６２０は、該ファイル６００の読み書き実行を利用者により制限するためのもので、該フ

ァイル６００の所有者以外の利用者に対する読込みの可／不可６２１、書き込みの可／不可６２２、実行の可／不可６２２が記述されている。利用者ＩＤ６３０は、該ファイル６００の所有者を唯一に識別する。データ６４０は、文書等の各種のデータや実行可能な処理プログラムのデータ本体である。

【００４１】次に、タスク制御ブロックについて図８を用いて説明する。タスク制御ブロック８００は、ＯＳ４００により制御されている各タスク４００に対して一個づつ設けられ、該タスクを利用している利用者を識別する利用者ＩＤ８１０と該利用者ＩＤ８１０が有効か無効かを示すＩＤ有効フラグ８２０を格納する。ＯＳ４００は、タスク４０１の起動に際して、タスク制御ブロック８００を生成する。また、ＯＳ４００は、タスク４０１が終了，消滅すると同時に、対応するタスク制御ブロック８００を削除する。

【００４２】次に、暗証番号管理テーブルについて、図９を用いて説明する。暗証番号管理テーブル９００は、各利用者ＩＤ９１０と、該各利用者ＩＤ９１０に対して設定された暗証番号９３０との対応関係が格納される。

【００４３】次に、ウインドウ管理データについて図１０と図１７を用いて説明する。ウインドウ管理データ１０００には、ディスプレイ装置３０５の画面１７００上に表示されている各ウインドウ１７１０について、該ウインドウ１７１０を表示しているタスク４０１のタスク制御ブロック８００が記憶されている主メモリ３０２上のアドレス１０１０が記述されている。また、ディスプレイ装置３０５の画面１７００上でアクティブな状態で表示されているアクティブウインドウ（図１７の例では１７１０ｃ）を示すために、アクティブウインドウポインタ１０２０が、該アクティブウインドウ１７１０ｃに対応するタスク制御ブロック８００のアドレス１０１０が記述されているウインドウ管理データ１０００中の位置を示している。

【００４４】次に、入退室管理装置１１１の入退室処理について図１１，図１２，図１４を用いて説明する。入退室処理１１００は、利用者が入退室管理装置１１１のカードリーダ１１１ａ，ｂに、カード１１４より、利用者ＩＤを入力すると（１１０１）、入退室管理テーブル１２００を更新し（１１０２）、入退室があったことを示すデータを、装置管理テーブル１１５０に記述されている各装置ＩＤ１１５５に対応する情報処理装置１１０に送信する（１１０３）。装置管理テーブル１１５０は、各情報処理装置１１０を唯一に識別するＩＤを複数格納することができ、一般には、該部屋１００内に設置されている各情報処理装置１１０と無線通信装置１１２の装置ＩＤ１１５５を格納する。これにより、以下で述べる利用者の入退室に関係する機密保護機能は、該部屋１００内に設置されている情報処理装置１１０～１１２の不正使用防止に限られる。但し、入退室管理装置１１１を出退勤管理に使用する例も考えられ、その場合は部屋１００とは関係無く、従業員の使用する各情報処理装置の装置ＩＤを装置管理テーブル１１５０に記述することにより、他人が既に退勤している従業員の利用者ＩＤを用いて該情報処理装置１１０を不正使用することが防止できる。また、部屋１００内のカードリーダ１１１ａにより、入力が行われた場合は退室と判断し、部屋１００外のカードリーダ１１１ｂにより、入力が行われた場合は入室と判断する。入退室管理テーブル１２００は、各利用者ＩＤ１２０１に対する入退室状況（入室中／退室後）１２０２が記述される。つまり、入室があった利用者ＩＤ１２０１の入退室状況１２０２には入室と記述され、退室があった利用者ＩＤ１２０１の入退室状況１２０２には退室と記述される。なお、入退室処理１１００は、制御処理１４００により、カードによる入力があった場合に起動される（１４１０，１４３０）。

【００４５】次に、入退室管理装置１１１の入退室状況問い合わせ処理について、図１２，図１３，図１４を用いて説明する。入退室状況問い合わせ処理１３００は、制御処理１４００により、他の情報処理装置１１０から、ある利用者が入室中か否かを問い合わせるデータを受信した場合に起動される（１４１０，１４２０）。入退室状況問い合わせ処理１３００は、まず、問い合わせの対象となる利用者ＩＤを受信し（１３２０）、該利用者ＩＤ１２０１に対応する入退室状況１２０２を入退室管理テーブル１２００から取得する（１３２０）。そして、該入退室状況１２０２を問い合わせ元の情報処理装置１１０に返信する（１３３０）。

【００４６】次に、機密保護設定画面について図１５を用いて説明する。機密保護設定画面１５００は、利用者が、ファイル６００に対して、他人の読込み，書込み，実行を禁止する保護属性を設定するための画面である。そして、機密保護設定画面１５００は、図１７に示すように、一つのウインドウ１７１０としてディスプレイ装置３０５の画面１７００上に表示される。また、この画面１５００は、例えば文書の編集終了時等、文書データをファイル６００として格納するときや、利用者が該ファイル６００に機密保護の設定を要求した場合に表示される。また、利用者が既存のファイル６００に対して、機密保護の設定または解除を要求した場合にも表示される。そして、該ファイル６００において他人の読込みを禁止する場合は、選択項目１５１５をマウス３０７を用いて指示する。一方、他人の読込みを許可する場合は、選択項目１５１０を指示する。また、他人の書込みを禁止する場合は、選択項目１５２５をマウス３０７を用いて指示する。一方、他人の書込みを許可する場合は、選択項目１５２０を指示する。また、他人の実行を禁止する場合は、選択項目１５３５をマウス３０７を用いて指示する。一方、他人の実行を許可する場合は、選択項目１５３０を指示する。さらに、後に述べるロック状態で

は、利用者ＩＤ１５４０と暗証番号１５５０の入力欄が表示され、利用者による利用者ＩＤと暗証番号の入力を必要とする。

【００４７】次に、アンロック画面について図１６を用いて説明する。アンロック画面１６００は、利用者が自分以外の人の読込みまたは書込みを禁止されているファイルを利用する時に、情報処理装置１１０に該利用者の利用者ＩＤを通知することによって、該利用者の読込み，書込み、または、実行を可能にするため指示を行う画面である。そして、アンロック画面は、図１７に示すように、一つのウインドウ１７１０としてディスプレイ装置３０５の画面１７００上に表示される。１６１０は利用者ＩＤの入力欄、１６２０は暗証番号の入力欄であり、利用者による利用者ＩＤと暗証番号の入力を必要とする。

【００４８】次に、本文処理装置のディスプレイ装置３０５の画面上における表示の一例を図１７を用いて説明する。１７１０は各タスク４０１が表示するウインドウである。なお、ある時点においては、画面１７００上で一つだけのウインドウ１７１０がアクティブな状態となる。アクティブな状態とは、キーボード３０６またはマウス３０７による入力が、該ウインドウ１７１０に対して、つまり、該ウインドウ１７１０を表示しているタスク４０１に対して行われることを意味している。１７２０は、後に述べるアンロック操作によって表示されるアンロック表示であり、現在、ある利用者に対する読込み，書込み、または実行の禁止が解除されていることを示す。１７２１は、１７２０と同様のアンロック表示であり、表示中のウインドウ１７１０の中に１つ以上のアンロック表示１７２０が行われているウインドウ１７１０がある場合に表示される。各ウインドウ１７１０内のアンロック表示１７２０がウインドウの重なりにより見えなくなり、アンロック状態であることが分からなくなることを防止するために１７２１も表示する。上述の画面表示例では、アンロックの状態を示すために１７２０を表示したが、ウインドウ枠の色をアンロックの状態を示す特定の色に変える実施例も考えられる。

【００４９】次に、以上で述べたシステム構成からなる情報処理装置における、機密保護関係の処理について説明する。

【００５０】まず、ファイルアクセスを制限する機構について、図１８を用いて説明する。タスク４０１は、ファイルアクセスをＯＳ４００に要求すると、該ＯＳ４００のファイルアクセス処理５０２は、まず、ファイル６００のアクセスが許されるか否かの検査を行い（１８１０）、次に、ファイルアクセス（１８２０）を行う。アクセス許可検査処理１８１０は以下の処理を行う。まず、アクセスするファイル６００のファイル保護属性６２０と利用者ＩＤ６３０を取得し、該ファイル保護属性６２０の各属性６２１～６２３の何れかに不可の指定がある場合は、以下の処理を行う。すなわち、ファイルアクセスを要求したタスク４０１に対応するタスク制御ブロック８００のＩＤ有効フラグ８２０を参照し、該ＩＤ有効フラグ８２０が有効を示していたならば、該タスク制御ブロック８００の利用者ＩＤ８１０を取得する。そして、該利用者ＩＤ８１０とファイル６００の利用者ＩＤ６３０が一致しない場合は、ファイル保護属性６２０で不可が示されている種類のアクセスが禁止される。ファイル保護属性６２０で可が示されている種類のアクセスは可能である。なお、ＩＤ有効フラグ８２０が無効を示していたならば、ファイル保護属性６２０に関係無く、全ての種類のアクセスが可能である。

【００５１】次に、利用者指示によって起動されるアンロック機能について、図１９を用いて説明する。本実施例におけるアンロックとは、利用者が自分以外の人の読込み，書込み、または、実行を禁止した文書ファイルを利用する時に、情報処理装置１１０に該利用者の利用者ＩＤを入力することによって、該利用者の読込み，書込み、または、実行を可能にすることである。アンロック機能は、機密保護タスク４０１ｅのアンロック処理１９００とＯＳのアンロック処理５０４ａにより実現される。

【００５２】まず、機密保護タスク４０１ｅのアンロック処理１９００について説明する。アンロック処理１９００は、利用者がキーボード３０６上のアンロックキー５０７ａを押した場合に、ＯＳ４００によって起動される。アンロック処理１９００は、図１６に示すアンロック画面１６００をディスプレイ装置３０５の画面に表示し、利用者から利用者ＩＤと暗証番号の入力を受け付ける（１９１０）。次に、入室中以外の利用者によるアンロックを禁止するために、入退室管理装置１１１へ処理１９１０で取得した該利用者ＩＤの利用者が入室中であるか否かを問い合わせ、入室中以外の場合は処理を終了する（１９２０）。次に、暗証番号管理テーブル９００を参照し、１９１０の処理で入力された利用者ＩＤと暗証番号の対応関係が、該暗証番号管理テーブル９００に記述されている利用者ＩＤ９１０と暗証番号９３０の対応関係と一致しているか否かを検査する（１９３０）。不一致の場合は処理を終了し、一致している場合は、ＯＳ４００のアンロック処理を起動する（１９４０）。

【００５３】次に、ＯＳ４００のアンロック処理５０４ａについて説明する。ＯＳ４００のアンロック処理５０４ａは、ディスプレイ装置３０５の画面１７００上にアクティブな状態で表示されているウインドウ１７１０を表示しているタスク４０１に関してアンロックの処理を行う。機密保護タスク４０１ｅのアンロック処理１９００における１９４０の処理によって起動されたアンロック処理５０４ａは、まず、ウインドウ管理データ１０００を参照し、アクティブな状態で表示されているウインドウ１７１０を表示しているタスク４０１のタスク制御

ブロック８００のアドレス１０１０を取得する（１９５０）。次に、機密保護タスク４０１ｅの処理１９１０で入力した利用者ＩＤを該タスク制御ブロック８００の利用者ＩＤ８１０として設定し、また、ＩＤ有効フラグ８２０を有効に設定する（１９６０）。また、該アクティブな状態のウインドウ１７１０にアンロック表示１７２０，１７２１の表示１０２２を行う（１９７０）。

【００５４】上述の実施例では、アンロックキー５０７ａを押したとき、アンロックはアクティブな状態のウインドウ１７１０を表示しているタスク４０１に対して行われたが、アクティブな状態でないウインドウ１７１０に関してアンロックを行う場合は、アンロックを行おうとするウインドウ１７１０をアクティブな状態にして（アクティベイト）からアンロックキー５０７ａを押す必要がある。

【００５５】次に、利用者指示によって起動されるロック機能について、図２０を用いて説明する。本実施例におけるロックとは、先に述べたアンロックの逆の操作であり、読込み，書込み、または実行を禁止したファイル６００に対するアクセスを不可能にすることである。ロック処理５０５ａは、利用者がキーボード３０６上のロックキー５０７ｂを押した場合に起動されるＯＳ４００の処理である。ロック処理５０５ａは、まず、ウインドウ管理データ１０００を参照し、アクティブな状態で表示されているウインドウ１７１０を表示しているタスク４０１のタスク制御ブロック８００のアドレス１０１０を取得する（２１１０）。次に、該タスク制御ブロック８００に設定されている利用者ＩＤ８１０をクリア（一般利用者を示す利用者ＩＤをセットする）する。（１２２０）。また、該アクティブな状態のウインドウ１７１０に表示されているアンロック表示１７２０を消去する。その際に、アンロック表示１７２０を行っている（アンロックの状態である）他のウインドウ１７１０がなければ、１７２１のアンロック表示も消去する。また、ウインドウ１７１０をクローズすることにより、該ウインドウ１７１０を表示しているタスク４０１を終了すると、ＯＳ４００が該タスク４０１に対応するタスク制御ブロック８００を削除する。

【００５６】上述の実施例では、ロックキー５０７ｂを押したとき、ロックは、アクティブな状態のウインドウ１７１０を表示しているタスク４０１に対して行われたが、アクティブな状態でないウインドウ１７１０に関してロックを行う場合は、ロックを行おうとするウインドウ１７１０をアクティブな状態にして（アクティベイト）からロックキー５０７ｂを押す必要がある。

【００５７】次に、入退室管理装置１１１が利用者の退室を検出し、そのことを各情報処理装置１１０に通知した場合の各情報処理装置１１０のロック処理について、図２１を用いて説明する。情報処理装置１１０が入退室管理装置１１１から退室データを受信すると、ＯＳ４００は、ロック処理５０５ｂを起動する。ロック処理５０５ｂは、まず、退室した利用者の利用者ＩＤを取得し（２１１０）、該利用者ＩＤと同一の利用者ＩＤ８１０を有する全てのタスク制御ブロック８００のＩＤ有効フラグ８２０を無効に設定する（２１２０）。そして、ディスプレイ装置３０５の画面１７００上に表示されているアンロック表示１７２０を消去する（２１３０）。

【００５８】次に、入退室管理装置１１１が利用者の入室を検出し、そのことを各情報処理装置１１０に通知した場合の各情報処理装置１１０のアンロック処理について、図２２を用いて説明する。情報処理装置１１０が入退室管理装置１１１から入室データを受信すると、ＯＳ４００は、アンロック処理５０４ｂを起動する。アンロック処理５０４ｂは、まず、入室した利用者の利用者ＩＤを取得し（２２１０）、該利用者ＩＤと同一の利用者ＩＤ８１０を有する全てのタスク制御ブロック８００のＩＤ有効フラグ８２０を有効に設定する（２２２０）。そして、ディスプレイ装置３０５の画面１７００上にアンロック表示１７２０を表示する（２２３０）。

【００５９】次に、機密保護設定処理について図２３を用いて説明する。機密保護設定処理２３００は、ファイル６００に対して他人の読書き実行を制限することを利用者が要求した場合に呼び出される。機密保護設定処理２３００は、まず、ウインドウ管理データ１０００を参照し、アクティブな状態で表示されているウインドウ１７１０を表示しているタスク４０１のタスク制御ブロック８００のアドレス１０１０を取得する（２３１０）。次に、該タスク制御ブロック８００に設定されている利用者ＩＤ８１０を参照する（２３２０）。そして、図１５に示した機密保護設定画面１５００を表示し、利用者が入力したファイル保護属性１５１０～１５３５、利用者ＩＤ１５４０、暗証番号１５５０を取得し（２３３０）、ファイル保護属性と利用者ＩＤをファイル６００の利用者ＩＤ６３０に設定する。但し、２３３０の処理は、該タスク制御ブロック８００に設定されている利用者ＩＤ８１０が、一般利用者を示す利用者ＩＤである場合のみ、利用者ＩＤの入力欄１５４０と暗証番号の入力欄１５５０を表示し、利用者に入力を要求する。それ以外の場合は、２３４０の処理でファイル６００に設定される利用者ＩＤ６３０は、２３２０の処理で取得したタスク制御ブロック８００の利用者ＩＤ８１０である。

【００６０】上述の各実施例では、アンロックキー５０７ａの押下時に、アクティブな状態にあるウインドウ１７１０を表示しているタスク４０１に関してのみアンロックを行ったが、該情報処理装置１１０で動作する特定の一部分または全てのタスク４０１に関してアンロックを行う実施例も考えられる。この場合、利用者は、アンロックを行った後、該情報処理装置で動作する全てのタスク４０１の利用に関して、該利用者以外に対してアクセス制限のあるファイル６００がアクセス可能となる。

また、この場合は、ロックは、該情報処理装置１１０で動作する特定の一部分または全てのタスク４０１に関してロックを行う。

【００６１】以上で述べた実施例によれば、情報処理装置１１０における利用者に対する機密保護状態の解除（アンロック）、及び、機密保護状態の設定（ロック）を、タスク４０１の実行中など利用者が希望する任意の時点で行うことを可能にし、機密保護状態が設定（ロック）されている状態では、アクセスが禁止されているファイル６００へのタスク４０１のアクセスを禁止することで、特定の利用者のアクセスのみが許されるファイル６００を使用する利用者に適した簡便な操作と、利用者によるアクセスの制限がないファイル６００を使用する一般利用者に適した簡便な操作とを両立した機密保護機能の操作方法を実現することができる。また、該ロック，アンロック機能を情報処理装置１１０が設置されている部屋１００の入退室管理機能と組み合わせることにより、他人が退室した人の利用者ＩＤを用いて情報処理装置１１０を不正に使用することを防止することができる。

【００６２】また、以上の実施例を改良した次のような実施例も考えることができる。

【００６３】まず、各タスク制御ブロック８００に、複数組の利用者ＩＤ８１１とＩＤ有効フラグ８２１を格納できるようにする。また、図１８に示したアクセス許可検査処理１８１０においては、タスク制御ブロック８００を参照し、ＩＤ有効フラグ８２１が有効を示している全ての利用者ＩＤ８１１の中にファイル６００の利用者ＩＤ６３０と一致するものが無い場合に、ファイル保護属性６２０で不可が示されている種類のアクセスを禁止するようにする。但し、ファイル保護属性６２０で可が示されている種類のアクセスは可能である。なお、全てのＩＤ有効フラグ８２１が無効を示していたならば、ファイル保護属性６２０に関係無く、全ての種類のアクセスが可能である。また、図１９におけるタスク制御ブロックＩＤ設定の処理１９６０では、利用者ＩＤ８１１とＩＤ有効フラグ８２１を追記するようにする（既に記述されている利用者ＩＤ８１１とＩＤ有効フラグ８２１に重ね書きしない）。

【００６４】また、以上の実施例を改良した次のような第２の実施例がある。第一の実施例では、利用者の指示と、入退室をきっかけとしてアンロック／ロックを行ったが、次に示すようなイベントを、アンロック／ロックのきっかけとして、単独または併用して用いてもよい。

【００６５】図２６を用いて説明する。ロック処理５０５を起動する処理として、離席検出処理２６１０、初期画面表示処理２６２０、無入力検出処理２６３０、スクリーンセーバ表示処理２６４０がある。

【００６６】離席検出処理２６１０は、図２７に示す、情報処理装置１１０に設置された離席検出装置２７００が検出した利用者の離席状態が、予め定められた一定時間に達し、かつ、アンロック状態のタスクが存在する場合（ＩＤ有効フラグ８２０に有効が設定されているタスク制御ブロック８００がある場合）に、ロック処理５０５を起動する。これにより、利用者がロックの指示を行わずに離席しても、自動的にロック状態となり、他の利用者による不正操作を防止できる。離席検出装置２７００は、ディスプレイ装置３０５の前方にある物体との距離を防止する超音波測距装置であり、測定距離が予め定められている一定距離を超えた場合に、該情報処理装置１１０の利用者が離席したと判断する。初期画面表示処理２６２０は、その情報処理装置で実行可能な機能の一覧を表示し、実行する機能を選択する初期画面を表示している状態が、予め定められた一定時間に達し、かつ、アンロック状態のタスク４０１が存在する場合（ＩＤ有効フラグ８２０に有効が設定されているタスク制御ブロック８００がある場合）に、ロック処理５０５を起動する。初期画面とは、情報処理装置１１０の電源投入後最初に表示される画面１７００であって、該情報処理装置１１０で使用可能な機能の選択画面が表示される。利用者が情報処理装置１１０の操作を終了または中断する場合、該画面を表示した状態にして、該情報処理装置１１０を放置する場合が多い。よって、これにより、利用者がロックの指示を行わずに離席しても、自動的にロック状態となり、他の利用者による不正操作を防止できる。無入力検出処理２６３０は、キーボード３０６、マウス３０７の無入力状態が、予め定められた一定時間に達し、かつ、アンロック状態のタスクが存在する場合（ＩＤ有効フラグ８２０に有効が設定されているタスク制御ブロック８００がある場合）に、ロック処理５０５を起動する。これにより、利用者がロックの指示を行わずに離席しても、自動的にロック状態となり、他の利用者による不正操作を防止できる。スクリーンセーバ表示処理２６４０は、焼き付き防止画面の表示開始と同時に、アンロック状態のタスクが存在する場合（ＩＤ有効フラグ８２０に有効が設定されているタスク制御ブロック８００がある場合）に、ロック処理５０５を起動する。これにより、利用者がロックの指示を行わずに離席しても、自動的にロック状態となり、他の利用者による不正操作を防止できる。なお、本第２の実施例は、以下で述べる実施例でも適用できる。

【００６７】また、以上の実施例を改良した次のような第３の実施例がある。第一の実施例では、利用者の指示や入退室等のイベントがあった時点でロック処理を行ったが、次に示すように、ある単位の処理が終了するまでロック処理の起動を保留してもよい。

【００６８】まず、予備制御テーブルについて、図２９を用いて説明する。予備制御テーブル２９００は各タスク制御ブロック８００に対応して設け、タスク制御ブロック８００と同様に、利用者ＩＤ２９１０とＩＤ有効フ

ラグ２９２０を設ける。

【００６９】つぎに、ロック一時保留機構について、図２８を用いて説明する。

【００７０】第一の実施例で述べた各ロック処理５０５において、タスク制御ブロック８００の利用者ＩＤ８１０を削除したり、ＩＤ有効フラグ８２０を無効に設定する処理では、第１の実施例でタスク制御ブロック８００に対して行ったのに代わって、予備制御テーブル２９００に対して行う。そして、アクセス制御データ整合処理２８００が、指定されたタスク４０１に対応する予備制御テーブル２９００に記述されている利用者ＩＤ２９１０とＩＤ有効フラグ２９２０の状態を、タスク制御ブロック８００に設定する。つまり、ロックが指示された時点では、タスク制御ブロック８００を操作してロック状態にしないで、アクセス制御データ整合処理２８００が動作した時点で、タスク制御ブロック８００を操作してロック状態にする。アクセス制御データ整合処理２８００は、図３０に示すように、3つの処理３０１０，３０２０から起動する場合が考えられる。各処理３０１０，３０２０からの起動を単独に用いても、併用しても良い。また、各処理３０１０，３０２０は、アクセス制御データ整合処理２８００を起動する際に、アクセス制御データ整合処理２８００の処理対象となるタスク４０１を唯一に識別するタスクＩＤを、パラメータとしてアクセス制御データ整合処理２８００に通知する。

【００７１】ファイルクローズ処理３０１０は、ＯＳ４００の処理であり、オープンしたファイル６００をクローズする処理を行う際に、アクセス制御データ整合処理２８００を起動し、ファイルのクローズを要求したタスクのタスクＩＤを、該アクセス制御データ整合処理２８００に通知する。

【００７２】タスク終了処理３０２０は、ＯＳ４００の処理であり、タスク４０１を終了する処理を行う際に、アクセス制御データ整合処理２８００を起動し、終了するタスクのタスクＩＤを、該アクセス制御データ整合処理２８００に通知する。

【００７３】第３の実施例では、ファイルのアクセスやタスクの処理が終了するまでロックの処理を一時保留することで、ファイルのアクセス中やタスクの実行中に利用者が退室したり、離席した場合にも、該ファイルのアクセスやタスクの実行が中断して異常終了となることを防止している。なお、本第３の実施例は、以下で述べる実施例でも適用できる。

【００７４】また、以上の実施例を改良した次のような第４の実施例がある。複数の利用者に対して同時に機密保護状態の解除（アンロック）を行うことが可能な実施例である。

【００７５】まず、各タスク制御ブロック８００に、複数組の利用者ＩＤ８１１とＩＤ有効フラグ８２１を格納できるようにする。また、図１８に示したアクセス許可検査処理１８１０においては、タスク制御ブロック８００を参照し、ＩＤ有効フラグ８２１が有効を示している全ての利用者ＩＤ８１１の中にファイル６００の利用者ＩＤ６３０と一致するものが無い場合は、ファイル保護属性６２０で不可が示されている種類のアクセスを禁止するようにする。但し、ファイル保護属性６２０で可が示されている種類のアクセスは可能である。なお、全てのＩＤ有効フラグ８２１が無効を示していたならば、ファイル保護属性６２０に関係無く、全ての種類のアクセスが可能である。また、図１９におけるタスク制御ブロックＩＤ設定の処理１９６０では、利用者ＩＤ８１１とＩＤ有効フラグ８２１を追記するようにする（既に記述されている利用者ＩＤ８１１とＩＤ有効フラグ８２１に重ね書きしない）。また、図２０で示したロック処理の代わりに、新たに図３２に示すロック処理を設ける。利用者によりロックキーが入力されたならば、機密保護タスク４０１ｅのロック処理３２００がＯＳ４００によって起動される。ロック処理３２００は、図３１に示すロック画面３１００を表示して、利用者によって利用者ＩＤ入力欄３１１０に入力される利用者ＩＤを取得した後、ＯＳ４００のロック処理５０５ａを起動する。ロック処理５０５ａは、まず、ウインドウ管理データ１０００を参照し、アクティブな状態で表示されているウインドウ１７１０を表示しているタスク４０１のタスク制御ブロック８００のアドレス１０１０を取得する（１９５０）。次に、該タスク制御ブロック８００に設定されている利用者ＩＤ８１０の中で、処理３２１０で取得した利用者ＩＤと同一の利用者ＩＤ８１１が記述されている利用者ＩＤ８１１とその有効フラグ８２１のフィールドを削除する（１９６０）。また、１９６０の処理を行った結果、各タスク制御ブロックについて、該タスク制御ブロック８００に記述されている利用者ＩＤ８１１が無くなった場合は、該タスクが表示しているウインドウ１７１０におけるアンロック表示１７２０を消去する（１９７０）。さらにその結果、アンロック表示１７２０を行っている（アンロックの状態である）ウインドウ１７１０が無くなれば、１７２１のアンロック表示も消去する。また、ウインドウ１７１０をクローズすることにより、該ウインドウ１７１０を表示しているタスク４０１を終了すると、ＯＳ４００が該タスク４０１に対応するタスク制御ブロック８００を削除するので、ロックと同じ効果がある。

【００７６】また、図２２で示した入室データ受信によるアンロック処理と、図２１で示した退室データ受信によるロック処理にも、同様な多重方式への変更を行う。つまり、図２２におけるタスク制御ブロック有効フラグセットの処理２２２０では、全てのタスク制御ブロック８００に関して、２２１０の処理で取得した利用者ＩＤと一致する全ての利用者ＩＤ８１１に対応するＩＤ有効フラグ８２１を有効に設定する。また、図２１における

タスク制御ブロック無効フラグセットの処理２１２０では、全てのタスク制御ブロック８００に関して、処理２１１０で取得した利用者ＩＤと一致する全ての利用者ＩＤ８１１に対応する有効フラグ８２１のフィールドを無効にセットする。また、２１２０の処理を行った結果、各タスク制御ブロックについて、該タスク制御ブロック８００に記述されている利用者ＩＤ８１１の中で有効フラグ８２１が有効に設定されているものが無くなった場合は、該タスクが表示しているウインドウ１７１０におけるアンロック表示１７２０を消去する（２１３０）。さらにその結果、アンロック表示１７２０を行っている（アンロックの状態である）ウインドウ１７１０が無くなれば、１７２１のアンロック表示も消去する。

【００７７】この第２の実施例では、第１の実施例での効果に加えて、同一の情報処理装置１１０または同一のタスク４０１において、複数の利用者に対して同時に機密保護状態の解除（アンロック）を行うことができる。つまり、ファイルＡのアクセスが利用者Ａに許可されていて、ファイルＢのアクセスが利用者Ｂに許可されている場合、利用者Ａ，Ｂについてアンロックを行えば、ファイルＡとファイルＢのアクセスが同時に行える。これは、一人の利用者が、例えばＡ委員会メンバーとしての利用者ＩＤとＢ委員会メンバーとしての利用者ＩＤ等、２つ以上の利用者ＩＤを持つ場合の操作に便利方式である。グループＩＤを設ける方式もあるが、グループの再編分割、所属変更が頻繁に行われる場合は、本実施例のように、一人の利用者が２つ以上の利用者ＩＤを持てる方式の方が現実的に対処できる。

【００７８】また、以上の実施例を改良した次のような第５の実施例がある。同一のファイルアクセスに対して、二人以上の利用者に対する機密保護状態の解除（アンロック）を必要とするようにできる方式である。

【００７９】まず、図６に示したファイル６００のファイル保護属性６２０を、図２５に示す構造に変更し、図６の利用者ＩＤ６３０を廃止する。つまり、複数の保護属性６２５を記述できるようにし、各保護属性６２５には、連動属性６２４と一つ以上の利用者ＩＤ６２６を記述できるようにする。連動属性６２４には、連動／非連動の区別が記述される。連動と記述されている場合は、同一のファイル保護属性６２５に記述されている各機密保護属性６２１～６２３で不可と設定されているアクセスが可能になる状態は、情報処理装置１１０が同一のファイル保護属性６２５に記述されている全ての利用者ＩＤ６２６に対してアンロック状態になっている場合に限られる。一方、非連動と記述されている場合は、同一のファイル保護属性６２５に記述されている各機密保護属性６２１～６２３で不可と設定されているアクセスが可能になる状態は、情報処理装置１１０が同一のファイル保護属性６２５に記述されているいづれかの利用者ＩＤ６２６に対してアンロック状態になっている場合である。そして、第１の実施例において、図１８で示したファイルアクセス制限機構のアクセス許可検査１８１０を、上述のファイル保護属性６２０に適合するように変更する。

【００８０】この第５の実施例では、あるファイルのアクセス（特に、処理プログラムが格納されているファイルの実行）に際して、複数の利用者に対してアンロック状態とすることを必要とすることができる。つまり、例えば、工業プラントの始動等、そのファイル（処理プログラム）の実行が重大な結果を生む可能性のある場合、一人の軽率な判断でなく複数の利用者の判断の下での実行を要求し、システムの安全性を高めることができる。

【００８１】

【発明の効果】以上述べたように、本発明によれば、情報処理装置の利用者に対する機密保護状態の解除（アンロック）、及び、機密保護状態の設定（ロック）を、利用者が希望する任意の時点で行うことを可能にし、また、該情報処理装置が設置されている部屋への利用者の入退室や、該情報処理装置の操作の中断とリンクして、ロックとアンロックを行う。そして、ロックされている状態では、アクセスが禁止されているファイルのアクセスを禁止することで、ファイルの不正利用を防止することができる。

【図面の簡単な説明】

【図１】システムの使用環境説明図である。

【図２】システム構成図である。

【図３】情報処理装置のハードウェア構成図である。

【図４】情報処理装置のソフトウェア構成図である。

【図５】情報処理装置の機密保護機構の説明図である。

【図６】ファイルのデータ構造の説明図である。

【図７】ファイル保護属性のデータ構造の説明図である。

【図８】タスク制御ブロックのデータ構造の説明図である。

【図９】暗証番号管理テーブルのデータ構造の説明図である。

【図１０】ウインドウ管理データのデータ構造の説明図である。

【図１１】入退室管理装置の入退室処理の説明図である。

【図１２】入退室管理装置における入退室管理テーブルのデータ構造の説明図である。

【図１３】入退室管理装置の入退室状況問い合わせ処理の説明図である。

【図１４】入退室管理装置の制御処理の説明図である。

【図１５】機密保護設定画面の表示例を示す図である。

【図１６】アンロック画面の表示例を示す図である。

【図１７】ディスプレイ装置の画面表示例を示す図である。

【図１８】ファイルアクセス制限機構の説明図である。

29

【図１９】利用者指示によるアンロック処理の説明図である。

【図２０】利用者指示によるロック処理の説明図である。

【図２１】退室データ受信によるロック処理の説明図である。

【図２２】入室データ受信によるアンロック処理の説明図である。

【図２３】機密保護設定処理の説明図である。

【図２４】第４の実施例に係るタスク制御ブロックのデータ構造の説明図である。

【図２５】第５の実施例に係るファイル保護属性のデータ構造の説明図である。

【図２６】第２の実施例に係るロック処理起動の説明図である。

【図２７】第２の実施例に係る離席検出装置の設置状況の説明図である。

30

【図２８】第３の実施例に係るロック一時保留機構の説明図である。

【図２９】第３の実施例に係る予備制御テーブルのデータ構造の説明図である。

【図３０】第３の実施例に係るアクセス制御データ整合処理起動の説明図である。

【図３１】第４の実施例に係るロック画面の表示例を示す図である。

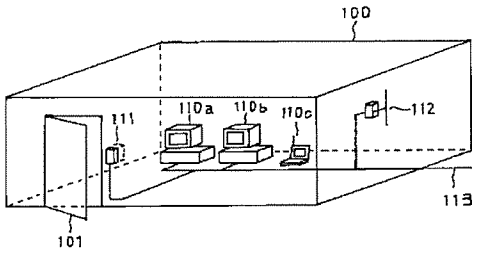
【図３２】第４の実施例に係る利用者指示によるロック処理の説明図である。

【符号の説明】

４００…ＯＳ、４０１ａ～ｂ…各種タスク、４０１ｅ…各種機密保護、５０１…ファイルアクセス要求、５０２…ファイルアクセス処理、５０３…アンロック要求、５０４…アンロック処理、５０５…ロック処理、５０６…データ受信、５０７…キー入力、６００…ファイル、８００…タスク制御ブロック。

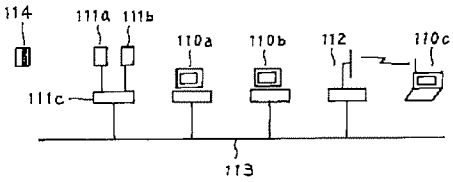
【図１】

図 1



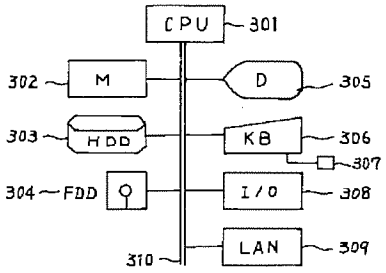
【図２】

図 2



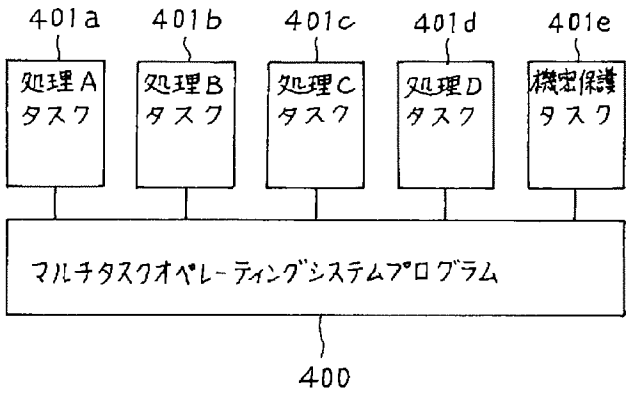
【図３】

図 3



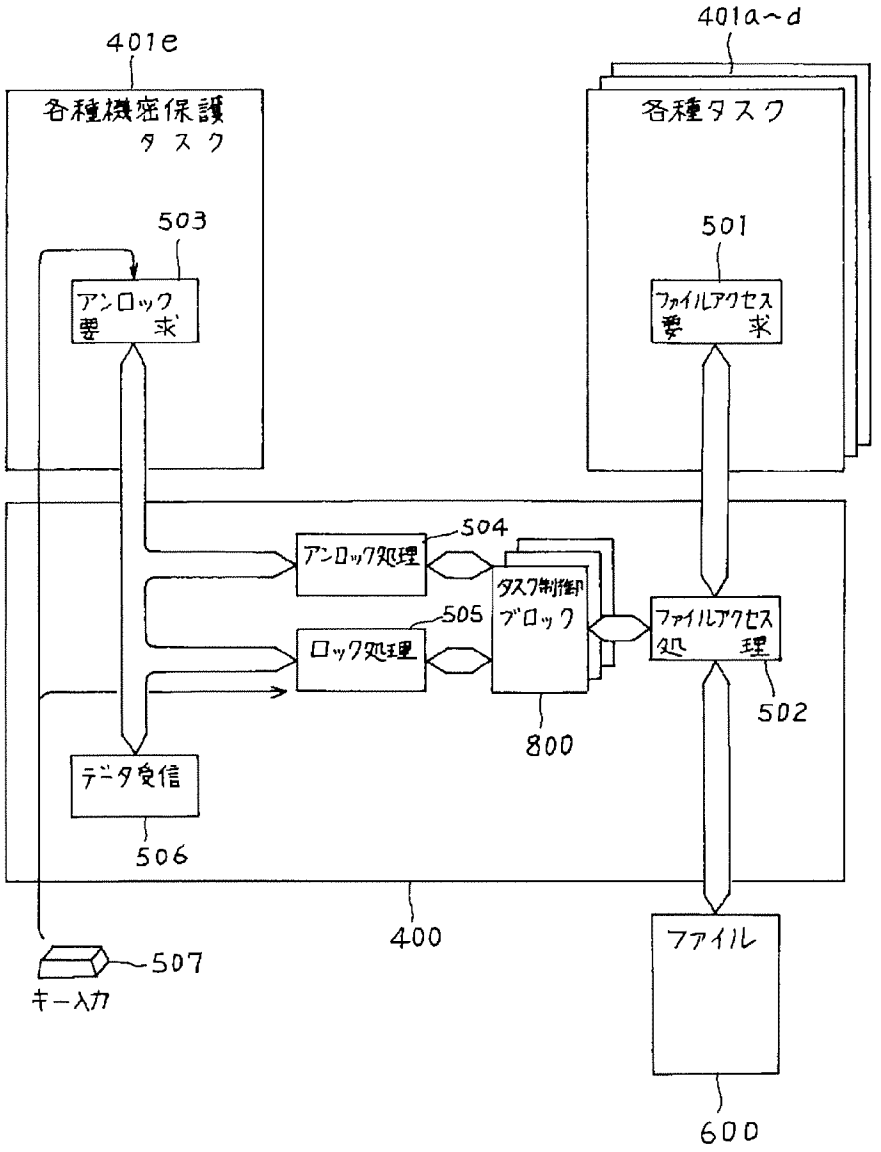
【図４】

図 4



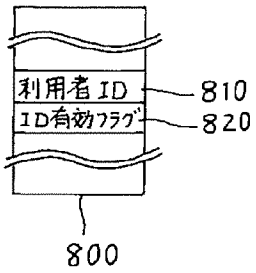
【図５】

図 5



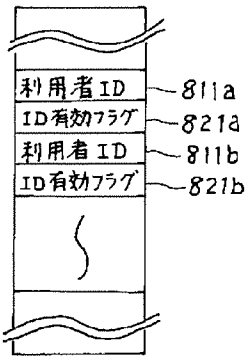
【図８】

図 8



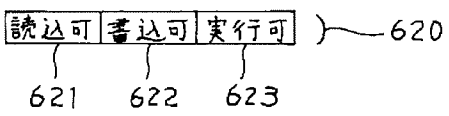
【図２４】

図 24



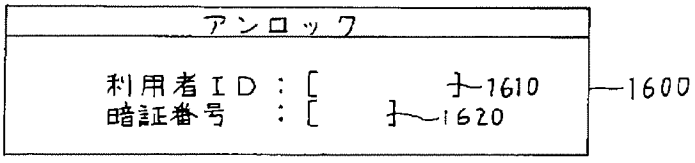
【図７】

図 7



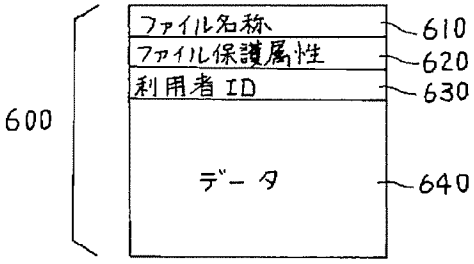
【図１６】

図 16



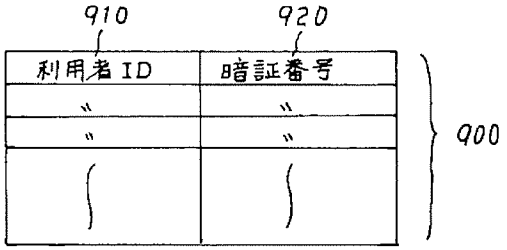
【図６】

図 6



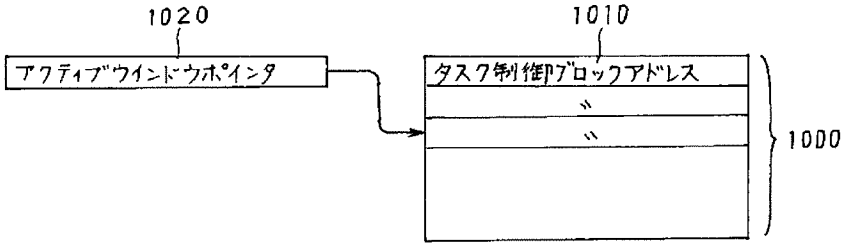
【図９】

図 9



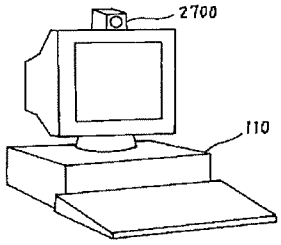
【図１０】

図 10



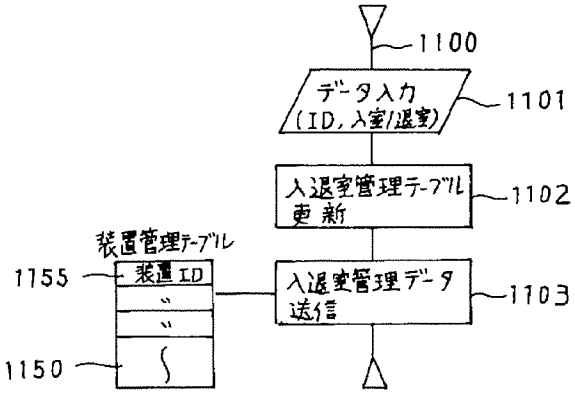
【図２７】

図 27



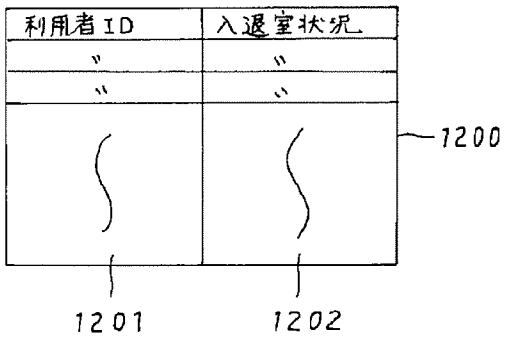
【図１１】

図 11



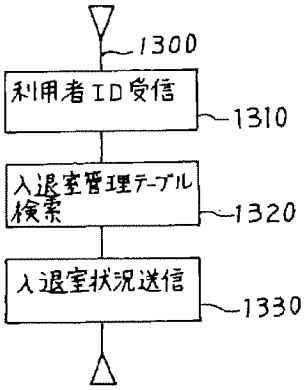
【図１２】

図 12



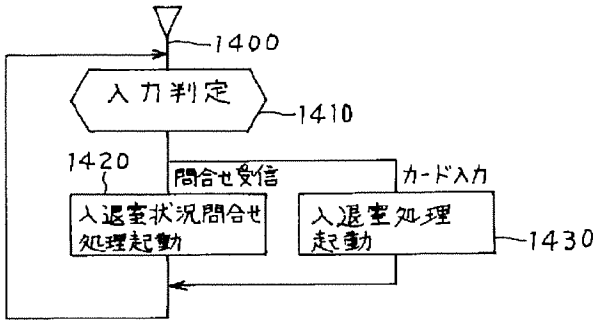
【図１３】

図 13



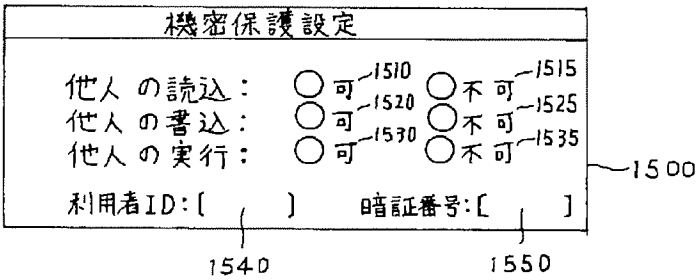
【図１４】

図 14



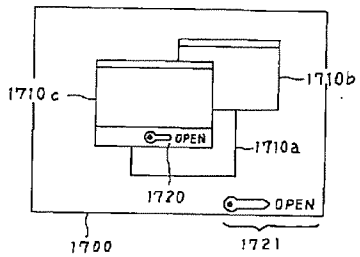
【図１５】

図 15



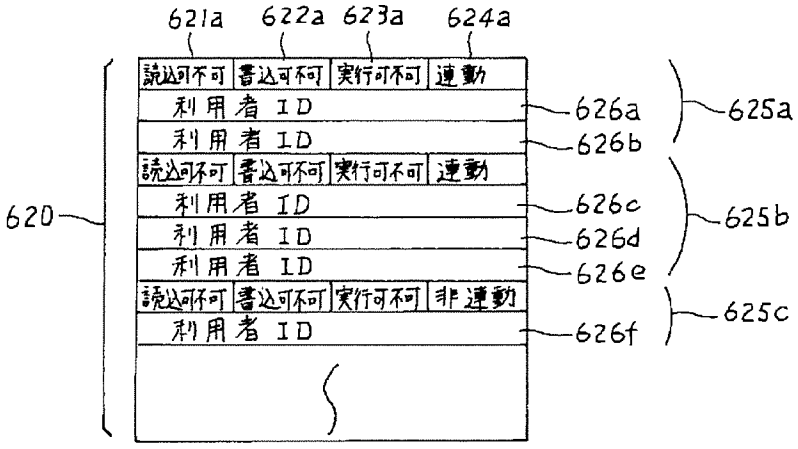
【図１７】

図 17



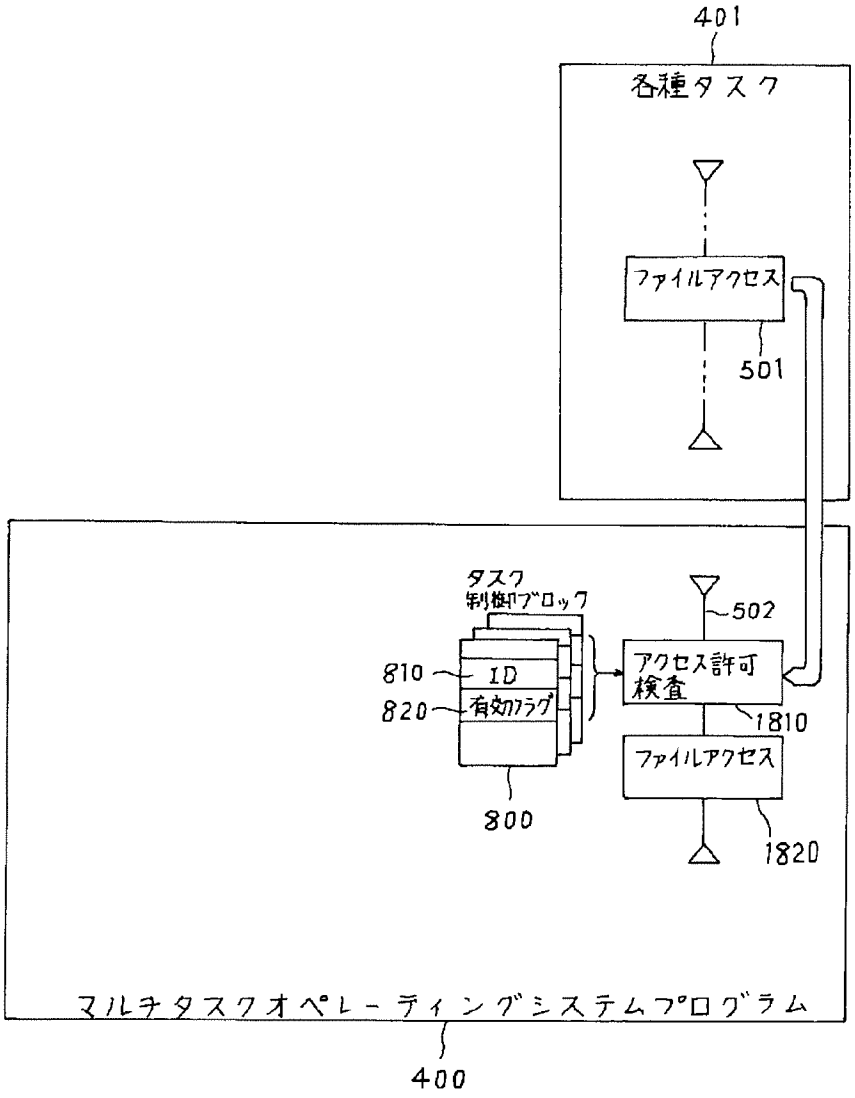
【図２５】

図 25



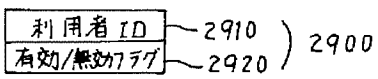
【図１８】

図 18



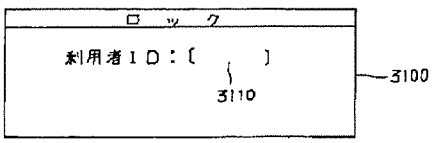
【図２９】

図 29



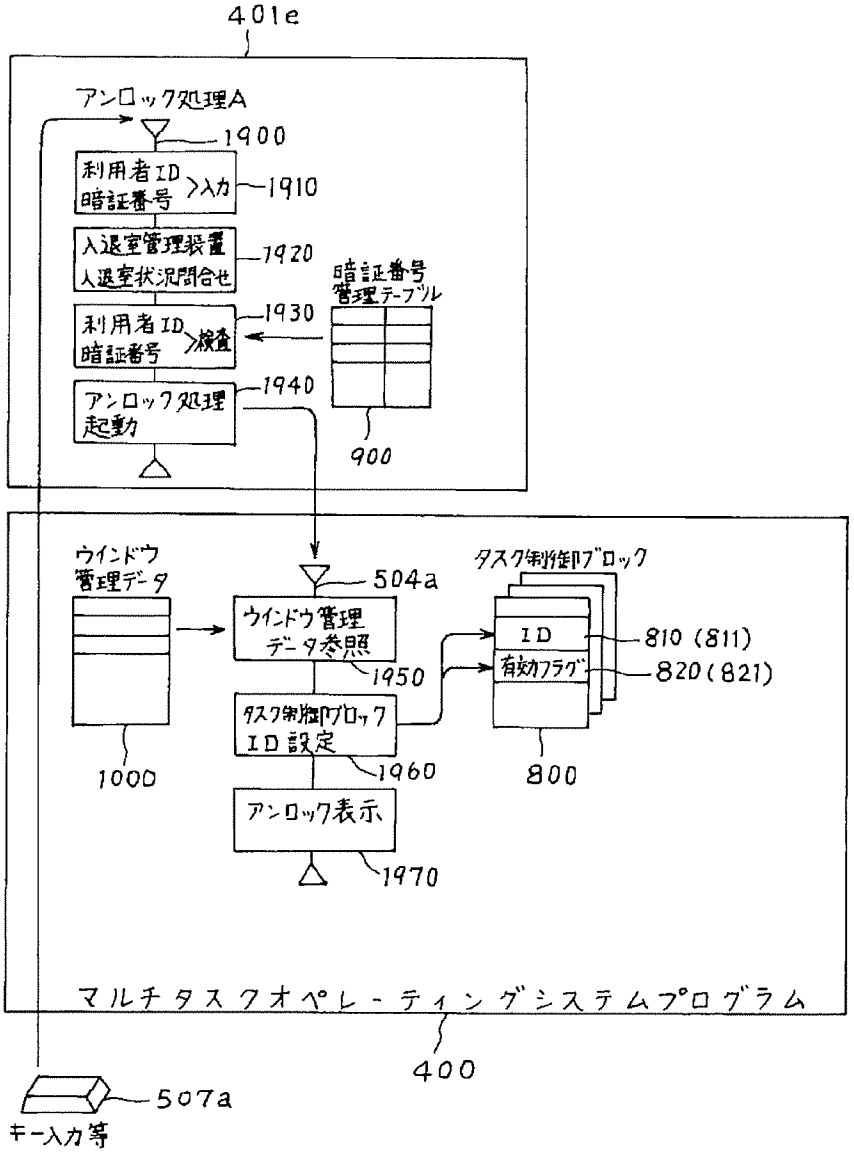
【図３１】

図 31



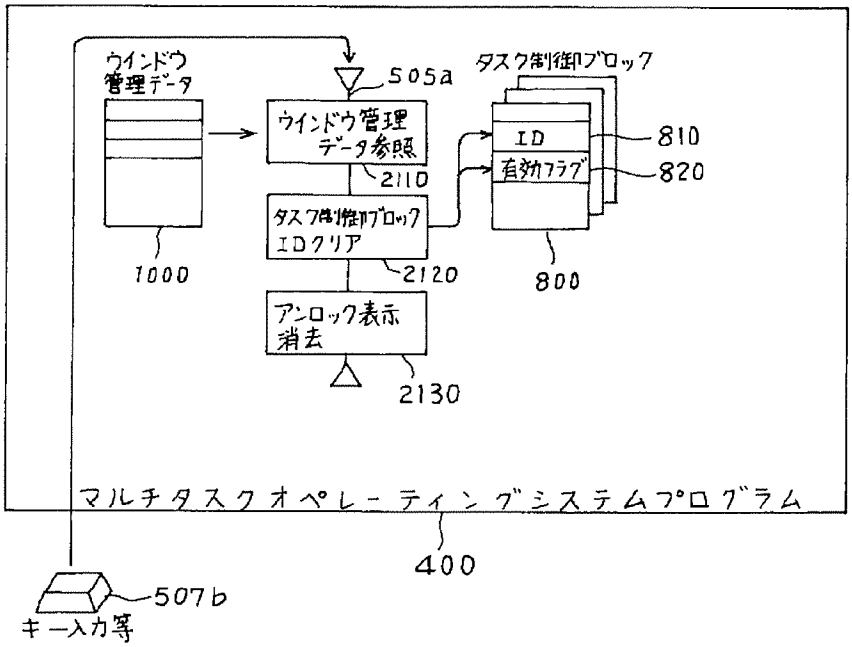
【図１９】

図 19


401e
アンロック処理A
1900
利用者ID
暗証番号
入力
1910
入退室管理装置
入退室状況問合せ
1920
利用者ID
暗証番号
検査
1930
暗証番号
管理テーブル
アンロック処理
起動
1940
900
ウインドウ
管理データ
504a
ウインドウ管理
データ参照
1950
タスク制御ブロック
ID設定
1960
アンロック表示
1970
タスク制御ブロック
ID
有効フラグ
810 (811)
820 (821)
800
1000
マルチタスクオペレーティングシステムプログラム
400
507a
キー入力等

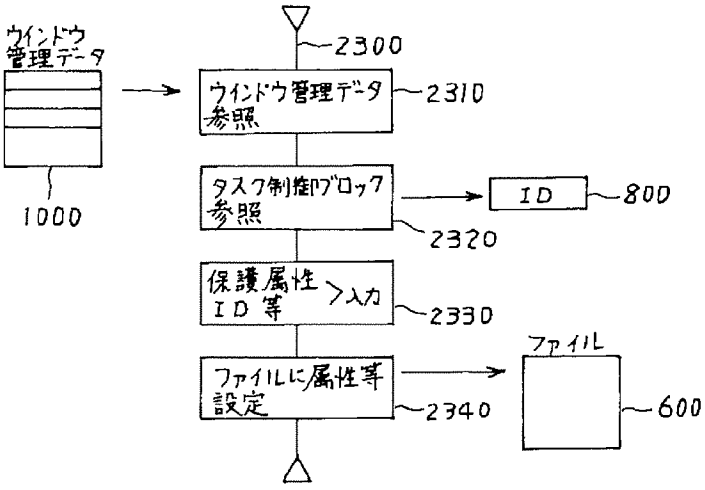
【図２０】

図 20



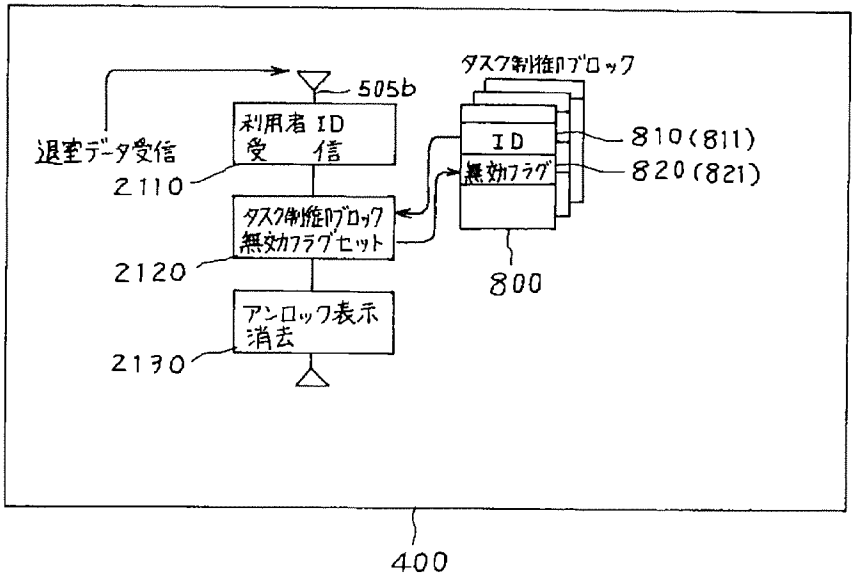
【図２３】

図 23



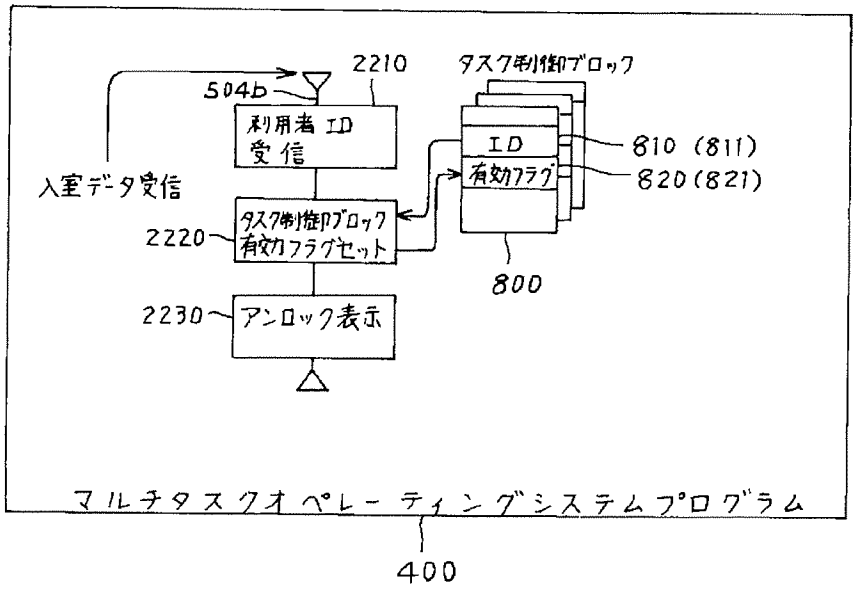
【図２１】

図 21



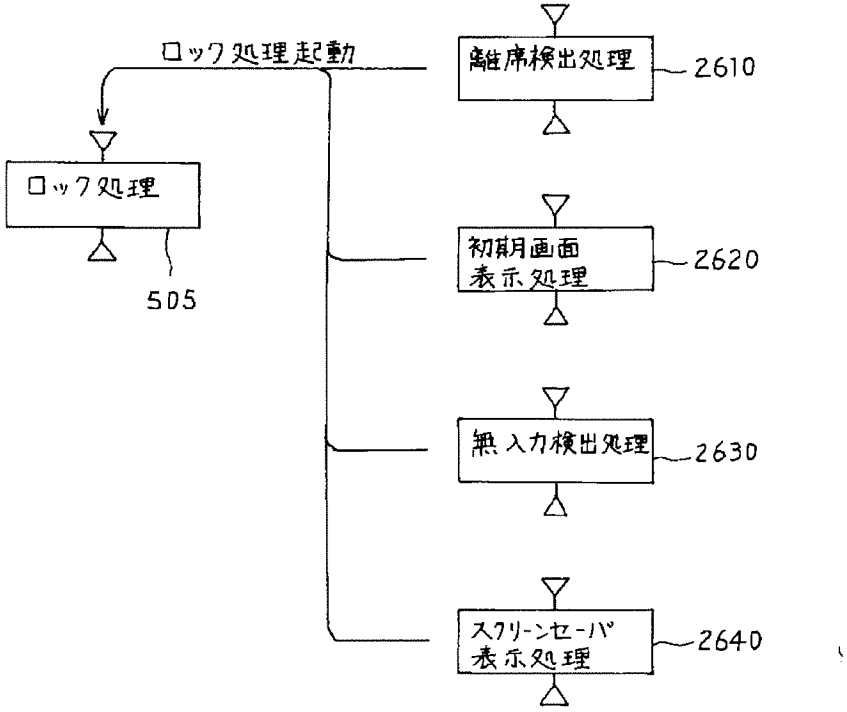
【図２２】

図 22



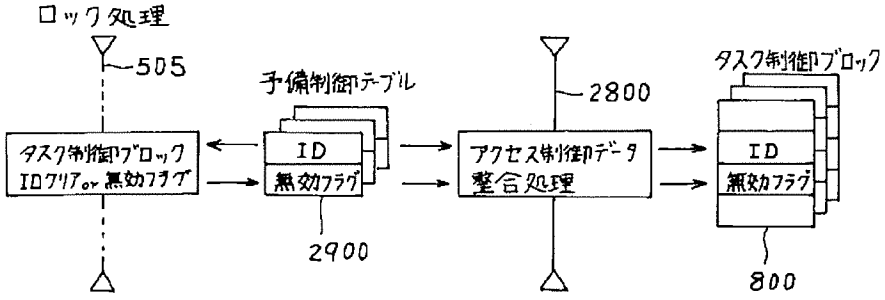
【図２６】

図 26



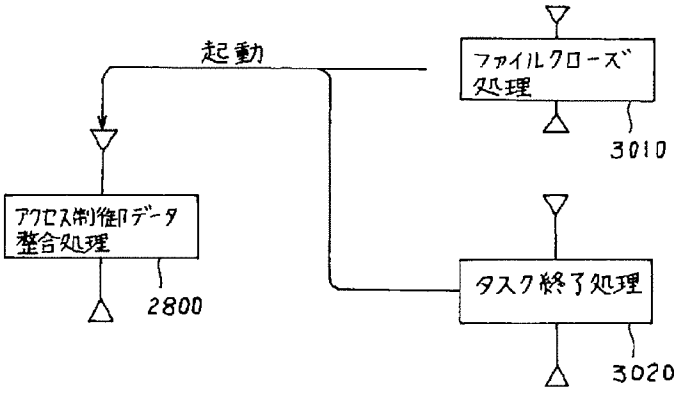
【図２８】

図 28



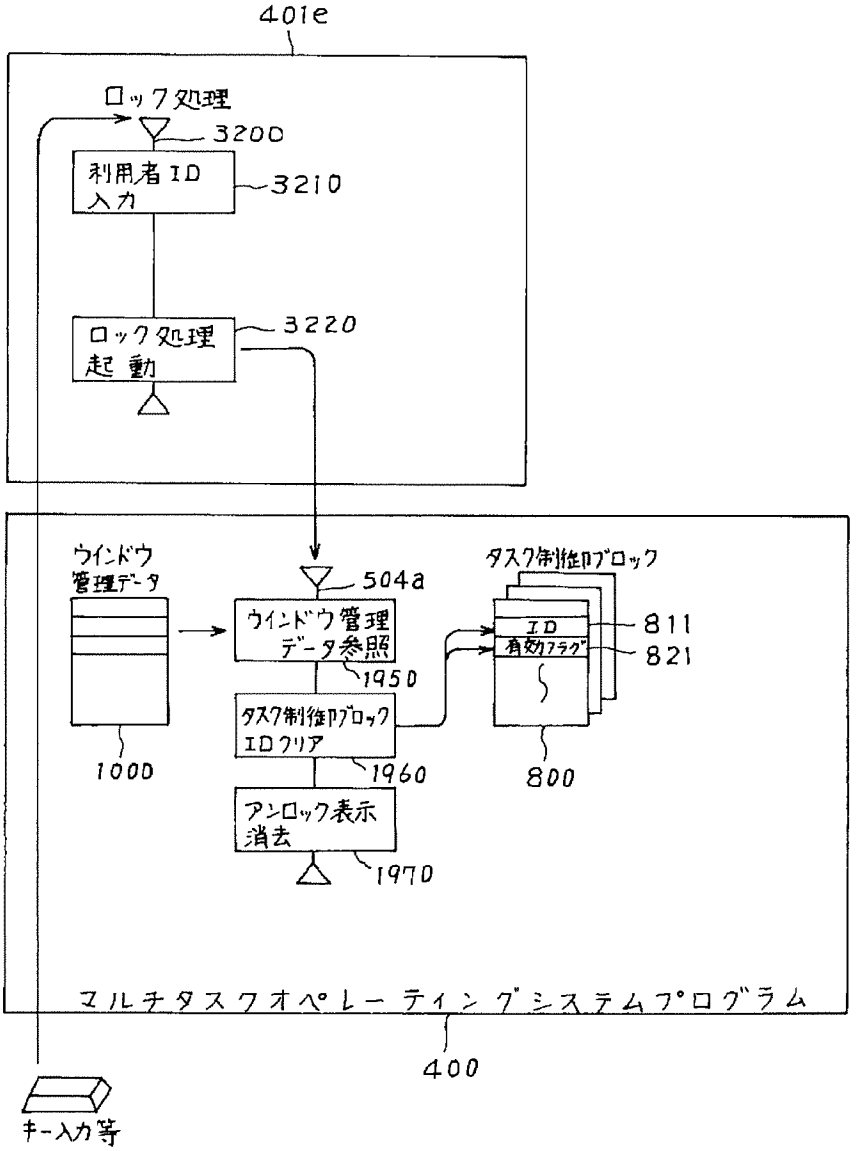
【図３０】

図 30



【図３２】

図 32



フロントページの続き

(72)発明者　尾崎　友哉
横浜市戸塚区吉田町292番地株式会社日立
製作所マイクロエレクトロニクス機器開発
研究所内